ISSN: 2450-6869

eISSN: 2719-6763

No. 13, 2022

DEFENCE SCIENCE REVIEW

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

DOI: 10.37055/pno/152385

The evolution of the concept of information warfare in the modern information society of the post-truth era

Original article

Received: 2022-07-06

Revised: 2022-08-03

Accepted: 2022-08-04

Final review: 2022-08-03

Peer review:

Double blind

Keywords:

information warfare, information society, disinformation, Russian Federation

Patrycja Bryczek- Wróbel[1,E,F]

ORCID 0000-0001-7154-7335

Maciej Moszczyński[1,D]

ORCID 0000-0003-3005-263X

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] Military University of Technology

Abstract

Objectives: Compare selected concepts of information warfare and show the evolution of the Western concept of WI,resulting from the development of the information society, social-media and the resources by which information warfare is conducted.

Methods: The research method used is a systematic review of Western political science literature, as well as military literature, publications on international relations, international politics, security and cyber security from the perspective of information warfare. Techniques such as analysis of background material, causal analysis and scientific and self-observation in this area were used, taking into account the dynamics of technological and geopolitical changes occurring in the modern information society.

Results: The analysis made it possible to show the evolution of the Western concept of information warfare and outline the main differences from the concept of information warfare adopted by the Russian Federation. The study also points out the threats to the information society posed by the realities of modern information warfare.

Conclusions: The Western conception of WI differs from that of the Russian Federation, placing the emphasis on WI as technological warfare, while the Russian Federation and the People's Republic of China (PRC) place the emphasis on psychological warfare first. This discrepancy could pose a significant threat to the information environment of Western democracies, since the weakest link in the security of not only an information system, but also an information system, is the human being. This is well known not only to hackers, cyber criminals, but also to hostile state or non-state forces that conduct WI against Western countries.

Corresponding author: Patrycja Bryczek Wróbel – Military University of Technology, ul. Kaliskiego 2, 00-908 Warsaw, Poland; email: patrycja.bryczek-wrobel@wat.edu.pl; Maciej Moszczyński- – Military University of Technology, ul. Kaliskiego 2, 00-908 Warsaw, Poland; email: maciej.moszczynski@wat.edu.pl

Introduction

The development of technology, communication tools and the spread of Internet access in the 21st century, have made the modern citizen of Western liberal democracies a citizen of not only an information society, but also a network society. This means that it has the technical ability to establish relationships with virtually any person (Castells, 2008, Kluszczyński, 2001). As Kennichi Koymama states in the information society, the main value for society is knowledge and information. In contrast, in a network society (which is one of the manifestations of the information society), the citizen becomes a node of a globalized network, who can establish an infinite number of relationships via the Internet, telephone (Goban-Klas, Sienkiewicz, 1999, Castells, 2008).

Every day, this "networked citizen" not only receives, but also creates and transmits terabytes of information within his circles of friends. Although he has virtually unlimited access to channels and sources of information acquisition, at the same time he has neither the time nor the developed skills to verify the onslaught and overwhelming digital information stream (data deluge) by which he cannot distinguish between lies and truth. This is well known not only by politicians, the media, private companies, but also by states and political blocs that recognize the potential (or necessity) of waging permanent information warfare to destabilize (or protect) the information society in order to achieve their desired political, economic and even military goals (Cronin & Crawford 2006).

The purpose of this paper is to show the evolution of the concept of information warfare and to try to reflect on whether contemporary concepts of information warfare fully reflect the nature of information warfare waged in the information space of Western liberal democracies.

1. The concept of information warfare in the 1990's

The Concept of Information Warfare in the 1990's. The concept of information warfare in Western liberal democratic states, dates back to the late 1980s. Initially, the concept was specific to the military field, as it was derived from electronic warfare, military deception, psychological operations and information-operational security (Libicki, 1996, Hutchinson, 2006). It has been understood to refer almost exclusively to the use of ICT to break into an adversary's ICT infrastructure in order to disrupt it or to gain relevant data and information about an adversary's resources, military strategies or defense of one's own infrastructure (Libicki, 1996, Endsley & Jones, 1997, Waltz, 1998).

Thus understood, WI was a tool used mainly to gain battlefield advantage, for example, by gaining superior performance in intelligence, targeting, command and control, among others. An example from the use of technology in information warfare included the 1991 Gulf War (Hutchinson, 2006, Campen, 1992). During Operation Desert Storm, troops of the international coalition completely dominated the Iraqi army in a technological information war, disrupting its communications, dominating the intelligence field and destroying its ICT infrastructure.

However, in addition to the components mentioned earlier, the development of an additional WI component of media management was evident in this conflict. These actions were the result of the experience of the so-called "defeat on the home front" during the Vietnam War, when unchecked media coverage led to the loss of the war off the battlefield, as a result of mass civil protests in the United States. The Vietnam conflict was the first to show liberal democracies the importance of controlling the media in influencing public opinion (Carruthers, 2000). Therefore, during the 1991 Gulf War, media representatives were carefully controlled and instructed to provide only information that was approved by either officials or the military (Taylor, 1992, Knightley, 2000, Hutchinson, 2006). This carefully planned and executed operation helped build a coherent narrative of the Gulf War as a just and humanitarian war.

Although media management was already an element of warfare, there was still no clear consensus on definitional grounds to include media management in the catalog of WI measures. For example, the 1995 US AIR FORCE definition defined WI as activities designed to deny, exploit, damage or destroy enemy information; protect against these activities; and exploit the military's own information functions. A much broader definition was given by Martin Libicki, who described WI as a collection of the following activities (Libicki, 1996):

- Command and control warfare - which aims to destroy or disrupt the enemy's command structure.
- Intelligence-based warfare - which uses smart sensors, smart weapons and combat information to make real-time decisions while preventing the enemy from doing so.
- Electronic warfare - which involves disrupting the adversary's transmission of information and protecting its own information from them.
- Psychological warfare - involving the development of information to directly influence public opinion, the military or commanders of enemy forces.

- Hacking war - involving attacks on computer information and control systems.
- Economic information warfare - involving attacks by blocking the flow of economic information, thereby controlling markets.
- Cyber warfare - involving a wide range of activities, from electronic terrorism (disrupting systems to cause havoc) to simulated war scenarios.

It should be added that in the 1990's there was another important change in the approach to information management. It was the redefinition of the very concept of information, which from a carrier of content became an autonomous, self-contained resource. This was due to the transition from the industrial era to the information and knowledge economy heralded by, among others, A. Toffler and P. Drucker (Drucker 1994, Kunder 2016), which forced organizations to transform their operating model based on labor, raw materials and capital into modern knowledge organizations.

This transition has led to the perception of information as a valuable resource to build advantage in economic and social struggles as well (Sveiby 1997, Drucker 1999, Asrar ul Haq and Anwar 2016). Thanks to this change in the perception of information, it began to be understood that information must be disseminated in a controlled manner not only during war, but also during peace.

2. The emergence of an oligopoly of media conglomerates and the development of media information warfare

The turn of the 20th and 21st centuries brought another important change for the information environment of Western liberal democracies. This was the development of global media companies that allowed them to create world media policy (such as CNN, Warner, Disney and Sony) by repeating information that came from official sources (Street, 2001, Hutchinson, 2006).

However, the change came not only in the increase in the spread of information, which could now promise the whole world through mass media, but also in the approach to its creation. The importance of mass media for achieving strategic goals began to be recognized. Particularly evident was the transformation in political struggles, which turned into spectacular "media clashes" that were a truly integrated and precisely planned process (Hutchinson, 2006). Clashes in which manipulation of information has become not only permissible, but necessary to achieve their strategic goals.

The result of this organized process of information warfare was the dynamic development of knowledge about influencing public opinion. Public relations techniques have

improved, and there has been an exponential increase in knowledge of information creation and dissemination, where empirical research, theories of social psychology and public diplomacy have begun to be applied to create effective strategies for manipulation and influence (Grunig et al. 2002, Batorowska et al. 2019, McKie, 2010). How effective the media could be used in waging information warfare is shown by the experience of the second Iraq war, which was the U.S. response to terrorist attacks on New York, Washington and Pensywlan. At the time, we were dealing with the complete domination of the military-prepared information perspective in the Western media. Only one official broadcast was present, in which very little controversial material was shown.

It can be echoed by Jean Baurillard that the second Iraq war "didn't happen" because the public didn't see the casualties and drama of the war, instead they were like a cinema viewer who watched a "Hollywood" production that was a show of special effects and explosions, using the effect of the so-called "sexiness of weapons" (Adie, 2004, Hutchinson, 2006). Repeating General Tommy Fransk , during the Iraq war the media became a fourth front. A front where information warfare was waged using pre-planned information messages programmed through means such as (Iyengar & Simon, 1994):

- Agenda setting - that is, the creation of significant events of the day that draw viewers' attention to certain desirable events, deliberately omitting what is inconvenient or contrary to the interests of the news broadcaster,
- Priming - which exploits the relationship between the patterns of news coverage and the criteria by which the public judges politicians, such that the media suggest to viewers the criteria that should be used to evaluate political actions,
- Framing - that is, the mass media programs the public's way of thinking by providing ready-made guidelines on how to interpret and evaluate reality.

During the second Iraq war, these means allowed the manipulation of public opinion by imposing a tense and broad agenda of the day's events that completely satisfied the public's appetite for information, pushing other, inconvenient information out of the public's consciousness. Moreover, each fact was properly prepared so as to increase the likelihood of its proper (expected by the sender) evaluation and promotion of the ideas desired by the information providers. Which is to say, it was presented in such a way as to pick out the desirable features of the events described and omit their other possible interpretations (Boisot, 1998, De Vreese, 2005). In addition, the democratic power took care not only of the message in the media corporations, but also on the Internet, creating custom-written blogs, accounts

and diaries of alleged witnesses to the war, who so never participated. The information campaign conducted in this way showed that the WI began to treat information as an instrumental tool for information warfare, in which not only techniques of manipulation and efficient use of information were used, but also its falsification and spreading disinformation.

3. Information Wars in Europe in the First and Second Decades of the 21st Century

The flywheel of subsequent changes in information management and processing was the spread of the Internet and the emergence of so-called social media, which enabled the partial transformation of the information society into a networked one. This is a society in which the network citizen becomes a node of the network, and information becomes the central value (Goban-Klas, Sienkiewicz, 1999, Castells, 2008). Thanks to the development of the Internet, the networked citizen can receive, create and transmit information faster than ever before. As a result, hundreds of millions of people have moved out of their cramped homelands and into the global "www village," where they can engage in anonymous social interactions and join online groups based on shared interests and values (Wagner, 1999, Barney, 2004). To use a comparison, one could say that the Internet has become to citizens of the 21st century network society what electricity was to industrial societies in the 20th century. Because it has changed people's lives in virtually every area - from shopping, to work, the private sphere and even the sexual sphere. In this society, technology has a dominant influence on its functioning, so significant that technology becomes society (Castells, 2008).

This diametric change in the way we communicate the processing, production and retrieval of information could not remain insignificant to the face of information warfare, which, like everything else in the digital age, sooner or later also had to move online. This relocation proved to be as rapid as the development of the Internet. As early as the time of the second Iraq war, it was noted that the Internet could serve as an effective complement to the mass media. Shortly thereafter, it was realized that it could be a much more effective tool than the media itself. As emphasized by M. Tadeo (Tkeshelashvili, 2021), information warfare began to be viewed as the use of information and communication technologies for offensive or defensive purposes to immediately invade, disrupt, or control an adversary's resources, and there were three major components within the definition of WI: deploying robotic weapons, carrying out cyberattacks and managing communications through information and communications technology. This has meant that WI has become the focus not only of the

military, but also of governments, information agencies, IT specialists and security experts (Tkeshelashvili, 2021).

WI has also begun to be understood as a broader concept than propaganda, encompassing a rich range of non-kinetic forms of interpersonal conflict, and the fact that information and communication technologies appear to be significantly cheaper, compared to the cost of traditional warfare, has been recognized as an asset (Taddeo, 2012, Tkeshelashvili, 2021).

What this new form of WI looked like was seen by Georgia during its 2008 conflict with the Russian Federation, when in addition to hostile coverage by pro-Russian media, it also had to contend with cyberattacks on government websites, e.g., on Aug. 11, an image collage of photos of the Georgian president and Adolf Hitler appeared on the Georgian parliament's website. Among the sites attacked were those of the Georgian Parliament, print media sites, "Rustavi 2" TV, the Tbilisi Forum site, the "Civil.Ge" news agency, and Georgian ministry sites.

In addition to jamming news broadcasts, Russia also built its own narrative, which called the bombing of airfields and military bases not a war, but an operation to coerce Georgia into peace. However, these actions were aimed not only at short-term disinformation and weakening the unity of society, but also at solidifying the FR's desired lines of thinking after the war:

1. Discrediting the ideas and sense of Georgia-EU and Georgia-NATO integration, presenting them as a threat to the territorial integrity of the state.

2. Stirring up negative attitudes in society toward Georgia's strategic partners, primarily the US and Turkey.

3. Promoting the role of Orthodoxy as a counterweight to Western, "rotten" and culturally alien values.

These new areas of WI activity showed that the concept of WI had to be liberated from strictly military connotations, since its activities in conflicts definitely go beyond the military. That's why, it has begun to be noticed that for modern WI it is no longer only the use of high technology and cyber warfare that matters, but also the use of journalists and the media (Cronin & Crawford, 1999, Lelonek, 2016). An example of the use of journalists and media in the WI is the 2014 conflict, where we saw a widespread disinformation campaign by the Kremlin not only against Ukraine, but also Western countries using not only traditional media, but also online media.

The Russians, with the help of so-called Internet trolls, state-controlled media outlets such as RT (the former Russia Today), Sputnik and Life News 4 conducted an organized

campaign in which the Kremlin argued that it had no intention at all to occupy Ukrainian territory and was not conducting any military operations. Initially, the message argued that the armed people were rebellious locals acting against the new government in Kiev, not invading troops. Subsequently, when it was known that the notorious green men had modern Russian equipment not excluding tanks and aviation, the Kremlin admitted the presence of its troops, but continued to deny the invasion of Ukraine, claiming that its purpose was solely to support harassed rebels who disagree with Kiev's Russophobic policies.

Of course, the essence of these actions was not only to create confusion in Ukraine, but also in Western public opinion, which received such contradictory messages that they could not tell whether Ukraine was at war, and even if information about the fighting reached them, it was impossible to say unequivocally who was the aggressor (Golovchenko et al. 2018).

This effectively made it difficult to accuse the Russian Federation of going to war, and consequently Western governments lacked sufficient legitimacy to take decisive action against Russia. The action proved so successful that General Philip Breedlove, NATO's Supreme Allied Commander in Europe, went so far as to call the Russian operation: "the most astonishing, most amazing blitzkrieg of information warfare we have ever seen in the history of information warfare."

This information blitzkrieg was based on massive operations not only in traditional media, but also on the Internet, as social media (e.g., Twittter, Facebook, VKontakte) became a virtual information battlefield. A particular example of this battle was the information war following the downing of a Malaysian Airlines plane (flight MH17), which killed 298 people.

The Russian side was building a narrative in which it blamed the crash on Ukrainian forces. Ukraine, on the other hand, with the support of international agencies, activists and independent journalists, was proving that the downing of the plane was not only the fault of the separatists who used the weapons, but also of their actual principals, the Russian government, since it was the latter who supplied them with the missile weapons used to destroy the plane. How important this clash was is evidenced by the fact that the publicizing of Russia's culpability led not only to the internationalization of the conflict in Ukraine, but also to the imposition of sanctions on Russia by the EU and NATO. Moreover, during the clashes of warring narratives on Twiter, Facebook or its Russian counterpart VKontakte, one could see the significant importance of either non-state institutions or individuals and groups of individuals who independently conducted disinformation or disinformation-fighting activities online (Golovchenko et al. 2018).

These activities have shown that in addition to the previously mentioned journalists or agents acting on behalf of states, a new soldier has emerged on the WI front, namely the Internet user. This is a soldier who can no longer only be a target, but also a means of conducting WI, since he is armed with a network of contacts and observers in social media allowing him to interact in the virtual community with a power equal to that of traditional media.

4. Information Warfare 2.0

Clashes in the Western information space on the part of the Russian Federation have proven that you don't have to be in an official state of war to fight in the information field. A prominent example was Russia's interference in the 2016 US presidential election, which included combined cyber and secret service activities (e.g., by funding the activities of political organizations), (Intelligence Community Assessment. Assessing Russian Activities and Intentions in Recent US Elections, https://www.dni.gov/files/documents/ICA_2017_01.pdf). Looking from a historical perspective, however, it can be said that attempts to destabilize Western democracies are nothing new for the Russians, as they stem from the Soviet doctrine of struggle against the imperialist West and the many concepts of action created for its use, such as the concept of so-called Maskirovka, which involves the use of deception, disinformation, secrecy, pretense, diversion, imitation, concealment, simulation and security in state actions (Shea, 2002, Hutchinson, 2006).

In order to understand the Russian Federation's actions in the modern information war, it is important to realize that, unlike Western states, a cynical approach to deception as an important factor in public-government and international relations in times of both peace and war for totalitarian regimes is perfectly acceptable and even desirable. Maskirovka's concept was that deception and trickery should be used in all areas of life and elements of politics regardless of time and circumstances. However, this approach does not stem from Soviet military thought but from Marxist logic, according to which socialist countries are always at war with countries of capitalist oppression (Vercellone, 2007). A state of war that has the nature of a permanent struggle along the lines of the Hobbesian state of nature, which makes it possible to justify every deception, every lie and every word in order to defeat evil and rotten Western capitalism, under the principle that the end justifies the means (Hutchinson, 2006).

Therefore, from the Russian perspective, WI is an activity designed to influence both the enemy's assessment of the military situation and the behavior of public opinion. One of the main tasks of WI in the Russian perspective is not to physically destroy the enemy only to subordinate its will to its own interests. Accordingly, WI can be treated on a par with conventional weapons and even nuclear troops and is a permanent war also in peacetime and cooperation (Darchaeva, 2016, Petkevich, 2018). Which was confirmed in the official foreign policy concept of the Russian Federation signed by Vladimir Vladimirovich Putin in 2016 and the concept of activities of the Armed Forces of the Russian Federation in the information space.

Along these lines, Russian doctrine has adopted a broad understanding of WI as integrated activities aimed at achieving a single strategy through, among other things:

- damage to information systems, processes and resources, critical structures and more,
- undermining political, economic and social systems,
- mass psychological attacks,
- psychological manipulation of the population to destabilize the state and society,
- forcing the state to make decisions favorable to the adversary.

One of the activities particularly targeted at Western societies are operations involving manipulation, propaganda and disinformation, which are aimed at obtaining so-called reflex control, which makes it possible, by giving a partner or opponent specially prepared information, to induce him to voluntarily make a predetermined decision desired by the initiator of the action (Thomas, 2004).

This wide range of integrated activities and the increasing encroachment on the information space of Western countries by the Russian Federation have forced the United States and allies to redefine their policies for securing the information environment and adapt them to new realities. There have been many attempts to define modern WI in the US (see Lopatina, 2014, Thornton, 2015, Lei, 2019, Di Pietro et al. 2021). First and foremost, earlier definitions have been expanded and supplemented to include both war and peacetime operations.

For example, according to a definition drafted for the US Congress, WI has been described as a broad range of military and government operations to protect and exploit the information environment, including both offensive and defensive activities that are conducted not only during emergencies and operational warfare, but also during peacetime. Whether government agencies, the media, or political leaders are under attack, the goal of these actions

is to influence either public opinion or decision-makers to take certain actions (Theohary 2018, Bolton, 2021).

These operations can consist of many different operational components (Bolton, 2021, Giles, 2016, p. 4, Libicki, 2017, pp. 49-50), which are used to support convoyed warfare operations such as:

- psychological operations - using propaganda and disinformation to win the hearts and minds of the enemy or weaken the opposition,
- electronic warfare - the use of technology to disrupt information networks and communication lines to degrade the ability to wage war,
- military deception and disinformation - misrepresentation in the military sphere
- cyberspace operations - protection of infrastructure, communication networks, information systems, etc.

Analyzing the sources, however, it is still apparent that WI has two worlds one western and the other eastern. Comparing the two, several important differences can be noted. First, Russian theorists, drawing on the tradition of the ZSSR emphasize active measures, having a much broader and more integrated approach to WI (Abrams, 2016, p. 8, Giles, 2016, p. 4, Bolton, 2021 p. 130). While the Russian Federation, like the West and the U.S., recognizes the importance of attacking an adversary's ICT networks and influencing or controlling the dissemination of information during conflicts - what they refer to as "information-technology warfare," they are far more appreciative of the importance of conducting WI aimed at societies and the psyche of citizens during peace (Giles, 2016 p. 6-9). Secondly, an important difference is the simultaneous interaction of actions on technological and psychological grounds to pursue centralized goals (Libicki, 2017, p. 50). Which means that the Russians will not retreat to attacks on critical infrastructure even of a country with which they are not officially at war, as exemplified by the massive cyberattacks on, for example, the Central Election Commission in Latvia during the 2018 elections, or the cyberattack on Estonia from April 27 to May 11, 2007 as retaliation for the relocation of a monument commemorating Red Army soldiers (Lapchinsky, 2009).

Conclusion

The analysis of selected definitions of WI conducted shows that the modern understanding of WI in the West differs from the definitions of the 1990’s and the first decade of the 21st century. The new definitions of WI in Western terms take into account new threats

in the information and cyber spheres. As a Western society, we have learned lessons from the Russian Federation's recent conflicts with Ukraine and Georgia and interference in the electoral process, so we understand that WI is a permanent struggle in both peacetime and war. Still, there is a different distribution of accents in the approach to WI between the East and the West.

The technologically advanced West places more importance on technology, while the concepts of both the FR and PRC emphasize strategic and psychological elements (Barrett 2005) treating the essence of WI as forcing an opponent to surrender without having to fight, such as by breaking his will to fight or misleading him about his own forces. To make matters worse, Western societies are still very susceptible to being influenced by their information environment because they are open information systems. By which disinformation, propaganda and psychological operations can more deeply penetrate Western social structures and shape public opinion than similar measures taken by the West against totalitarian regimes with hermetic, closed information circuits.

The Western approach to WI also fails to take into account the significant risks to citizens of an information and network society, where the problem is not only the easy availability of manipulated content, but also the lack of competence in properly evaluating it. One can see a certain discrepancy in preparations for conducting WI, on the one hand there is an emphasis on cyber defense through the creation of new barriers and safeguards that increase the ability of information systems to defend themselves passively, while on the other hand there is no effort of similar intensity to raise awareness among Internet users. And yet, the weakest link in the security of not only an IT system, but also an information system, is the human being, as not only hackers, cyber criminals, but also hostile state or non-state forces that conduct WI against Western countries know very well.

References

Asrar-ul-Haq, M. and S. Anwar (2016). "A systematic review of knowledge management and knowledge sharing: Trends, issues, and challenges." Cogent Business & Management 3(1).

Barney D. D. (2004): Społeczeństwo sieci. Warszawa: Wydawnictwo Sic!: s. 364.

Barrett Jr, B. M. (2005). Information Warfare: China's Response to US Technological Advantages. International Journal of Intelligence and Counterintelligence, 18(4), 682-706.

Batorowska, H., Klepka, R., Wasiuta, O. (2019). Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem: 327-378

Bolton, D. (2021). Targeting ontological security: Information warfare in the modern age. Political Psychology, 42(1), 127-142.

Boisot, M.H. (1998). Knowledge assets. Oxford: Oxford University Press.

Campen, A. D. (Ed.). (1992). The first information war: The story of communications, computers, and intelligence systems in the Persian Gulf War. Fairfax, VA: AFCEA International Press.

Carruthers, S.L. (2000). The media at war. Houndsville: MacMillan Press.

Castells, M. (2008). Społeczeństwo sieci. Warszawa: Wydawnictwo Naukowe PWN.

Cronin, B., Crawford H. (2006). Information Warfare: Its Application in Militaryand Civilian Contexts Available at: https://doi.org/10.1080/019722499128420

Cronin B., Crawford H. (1999). Information Warfare. Its Application in Military and Civilian Contexts, „The Information Society", Vol. 15, No. 4, Indiana University, Bloomington.

Darczewska, J. (2016). Russia's armed forces on the information war front. Strategic documents. Ośrodek Studiów Wschodnich im. Marka Karpia.

De Vreese, C. H. (2005). News framing: Theory and typology. Information design journal+ document design, 13(1), 51-62.

Di Pietro, R., Raponi, S., Caprolu, M., & Cresci, S. (2021). New Dimensions of Information Warfare. In New Dimensions of Information Warfare (pp. 1-4). Springer, Cham.

Drucker, P. F. (1999). Post-capitalist society: Science Publishing Company PWN, Poland.

Drucker, P. F. (1994). The Age of Social Transformation: The Atlantic Monthly 274: 27.

Endsley, M., Jones, W. (1997). Situation Awareness Information Dominance & Information Warfare. 94.

Goban-Klas, T., Sienkiewicz, P. (1999). Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania., Kraków: Wydawnictwo Postępu Telekomunikacji, s. 42.

Golovchenko, Y., Hartmann, M., & Adler-Nissen, R. (2018). State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation. International Affairs, 94(5), 975-994.

Grunig, L., Grunig, J., Dozier, D. (2002). Excellent Public Relations and Effective Organizations. Londyn: Mahwah.

Hutchinson, W., (2006). Information warfare and deception. Informing Science, 9, 213.

Iyengar, S., & Simon, A. (1994). News coverage of the gulf crisis and public opinion. In W. L. Bennett & D. I. Paletz (Eds.). Taken by storm – The media, public opinion, and U.S. foreign policy in the Gulf War (Ch. 8, pp.167 - 185). Chicago: University of Chicago Press.

Kluszczyński, R.W. 2001. Społeczeństwo informacyjne - Cyberkultura - Sztuka multimediów., Kraków: Rabid.

Knightley, P. (2000). The first casualty. Baltimore: John Hopkins University Press.

Kundera, E. (2016). Alvin Toffler's Concept of the Supersymbolic Economy. Economic Studies. Science Papers of the University of Economics in Katowice, Poland 259.

Lei, H. (2019). Modern information warfare: analysis and policy recommendations. Foresight.

Lelonek, A. (2016). Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowanie. W: Potencjaá sáowa. MiĊdzynarodowe stosunki i komunikacja: stan i perspektywy. Warszawa–Lwów: Fundacja Centrum BadaĚ Polska-Ukraina.

Libicki, M. (2017). The convergence of information warfare. Strategic Studies Quarterly, 11(2).

Libicki, M. (1996). What is Information Warfare? Washington, D.C, USA: National Defense University Press.

Lopatina, N. V. (2014). The modern information culture and information warfare. Scientific and Technical Information Processing, 41(3), 155-158.

Łapczyński, M. (2009). Zagrożenie cyberterroryzmem a polska strategia obrony przed tym zjawiskiem. Komentarz Międzynarodowy Pułaskiego, (7/09).

McKie, D. (2010). Signs of the Times: Economic Sciences, Futures, and Public Relations. W: „The Sage Handbook of Public Relations", Londyn.

Pietkiewicz, M. (2018). The military doctrine of the Russian Federation. Polish Political Science Yearbook, 47(3), 505-520.).

Russian Federation Armed Forces' Information Space Activities Concept (Moscow: Ministry of Defence of the Russian Federation, 2000).

Shea, T.C. (2002). Post Soviet maskirovka, cold war nostalgia, and peacetime engagement. Military Review, May/June, pp.63-67. Fort Leavenworth, Kansas: Command and General Staff College.

Street, J. (2001). Mass media, politics and democracy. Houndmills: Palgrave.

Sveiby, K. E. (1997). The New Organizational Wealth: Managing and Measuring Knowledge-Based Assets, Berrett-Koehler Publishers.

Taddeo, M. (2012). Information Warfare: A Philosophical Perspective, „Philosophy and Technology" 2012, vol. 25.

Taylor, P.M. (1992). War and the media: Propaganda and persuasion in the Gulf War. Manchester, UK: Manchester University Press.

Timothy L. Thomas, (2004) Russia's Reflexive Control Theory and the Military Journal of Slavic Military Studies 17: 237–256.

Tkeshelashvili, I. (2021). Rosyjska propaganda w przestrzeni informacyjnej Gruzji przed i po konflikcie w sierpniu 2008 roku. Wschodnioznawstwo, Tom 15: 55-71: DOI 10.4467/20827695WSC.21.003.14710.

Theohary, C. A. (2018). Information warfare: Issues for congress. Congressional Research Service, 7-5700.

Thornton, R. (2015). The changing nature of modern warfare: responding to Russian information warfare. The RUSI Journal, 160(4), 40-48.

Tkeshelashvili, I. (2021). Rosyjska propaganda w przestrzeni informacyjnej Gruzji przed i po konflikcie w sierpniu 2008 roku. Wschodnioznawstwo, Tom 15: 55-71: DOI 10.4467/20827695WSC.21.003.14710.

Vercellone, C. (2007). From formal subsumption to general intellect: Elements for a Marxist reading of the thesis of cognitive capitalism. Historical materialism, 15(1), 13-36.

Wagner, A. (1999). Life on the Screen: Identity in the Age of the Internet. The Psychohistory Review, 27(2), 113.

Waltz, E. L. (1998). Information Warfare Principles and Operations. Norwood, USA: Artech House, Inc.

Wojnowski, M. (2017). Paradygmat wojny i pokoju. Rola i znaczenie materializmu dialektycznego w rosyjskiej nauce wojskowej w XXI w. „Przegląd Bezpieczeństwa Wewnętrznego", nr 17, s. 41–43.

Electronic sources

Abrams, S. (2016). Beyond propaganda: Soviet active measures in Putin's Russia. Connections, 15(1), 5–31. https://doi.org/10.11610/Connections.15.1.01

Giles, K. (2016b). Handbook of Russian information warfare (Fellowship Monograph Series, No.9) Research Division NATO Defense College. Retrieved from https://krypt3ia.files.wordpress.com/2016/12/fm_9.pdf

Intelligence Community Assessment. Assessing Russian Activities and Intentions in Recent US Elections, https://www.dni.gov/files/documents/ICA_2017_01.pdf [dostęp: 17 06 2021].

Other sources

Adie, K. (2004). [Television presentation]. Press Club, Australian Broadcasting Corporation, 13.00hr, 22 December 2004.

The Foreign Policy Concept of the Russian Federation (Moscow: Ministry of Foreign Affairs, 2016).