HDR 2020, Nr. 2, 102–111.

Éva Ambrus

OF ENDS AND MEANS: THE INTEGRATION OF PSYCHOLOGICAL OPERATIONS AND CYBER OPERATIONS

DOI: 10.35926/HDR.2020.2.7

ABSTRACT: *Terminology is a general word for the group of specialized meanings relating to a particular field, encapsulating its meaning and intent. This article focuses on the evolving military terminology regarding psychological operations as technology moves forward. As a non-kinetic type of operation its content is more shifting, thus different terminologies are used, creating ambiguity. Furthermore, different concepts are behind as to what constitutes psychological operations. Words are important in naming the narrative and in this article, I will present a brief overview of this evolution and how it reflects on the present thinking – and it is a reflection of the organization of military forces.*

KEYWORDS: *Psychological operations, cyber operations, information operations, terminology*

INTRODUCTION

It is very probable that psychological warfare and psychological operations (further use: PSYOPS)[1] have been employed since the beginning of war and conflicts, albeit named differently. One example of this is the often quoted military theorist Sun Tzu, who advocated the psychological undermining of the enemy, often through demoralization.[2] The methods used through the ages were those available in society (rumour, printing, radio) and the development of psychological warfare has always been sensitive to the development of technology, as it rapidly adopts innovation to reach target audiences and influence outcomes. With the advances in info-communication technology, data analysis, public opinion analysis, and prediction of behaviours, psychological operations have become more systematic (data-driven) and widespread. As they have reached the boundaries of cyber domain, both of them benefitted from the synergies, and a convergence between cyber and information operations can be noted. Both of them are considered non-kinetic operation in Western military thinking and although non-kinetic operations rarely exist as a stand-alone concept, they are just as vitally important as kinetic operations in contemporary military operations.

[1] The U.S. terminology uses PSYOP whereas the NATO terminology is PSYOPS. In this article I use the latter.

[2] Post, J. M. "The key role of psychological operations in countering terrorism". In Forrest, J.J. F. (ed.) *Countering Terrorism and Insurgency in the 21st Century: Strategic and Tactical Considerations.* Westport: Praeger Security International, 2007. 380.

In this paper I present the different terminology involved in the discussion on psychological operations, cyber operations, and information operations. I focus on the transatlantic terminology, the overlaps and differences between them. These result in some confusion in the terms used in the literature. First I present a brief history of the term 'psychological operations', followed by the terminology and convergence of information operations, cyber operations, influence operations and information warfare, and finally contrasting it with the Russian concepts of combining information warfare elements.

BRIEF HISTORY

The first known application of the term 'psychological warfare' was in 1920 and 'psychological operations' in 1945 by British military analyst and historian, J.F.C. Fuller.[3] He stipulates that historically the used techniques are accepted as instruments of (furthering) national policy, "developing and refining Clausewitz's well known statement that *'war is a continuation of politics by other means'*."[4] The National Security Council (NSC) of the United States (US) viewed that psychological warfare techniques provide an additional way in which to conduct politics, both in peace and war, and it was a means to influence directly the people of foreign countries. Secondly, the NSC recognized the principle that psychological warfare – to be effective – must be a continuous process. During peace time it was called 'foreign information program', and the over-riding objective was to promote the understanding of US objectives and during war, the process is called 'psychological warfare'.[5]

These two principles, notably that psychological warfare deals not only with governments but directly with people and that it is a continuous process, are quintessential, even though the use of psychological warfare fell out of preference as the terminology often includes targeting neutral or even friendly audiences and thus the more neutral term 'psychological operations' became more prominent. With the technological advances of the last decades, first information operations and later cyber operations emerged.

These changes not only supported existing structures, but "since the 1990s, many political scientists […] have identified and advocated information as a fourth element of power [as] the dynamic security environment that we confront today and that in the future will alter the relative utility of the other three elements – economic, diplomatic and military".[6] The technological boom of the 2000s further divided the notion and with the emergence of new technologies, new 'operations' were created, thus creating confusion in the terms and definitions. With the more proponent spreading of the element of information warfare (IW), Libicki argues that a convergence of these notions can be seen.[7] In his view, three circumstances support the synergies between PSYOPS and CYBEROPS: first (1) they both may

[3] Daugherty, W. E. "Origin of Psyop Terminology". In Mclaurin, R. D. (ed.) *Military Propaganda: Psychological Warfare and Operations.* New York: Praeger Publishers, 1987. 257.

[4] Smith, C. H. "Psychological Warfare". *Naval War College Review* 6/2. 1953. 41.

[5] Smith."Psychological Warfare". 41.

[6] Jones, F. L. "Information: the psychological instrument". In Bartholomees, J. B. (ed.), *U.S. Army War College guide to national security policy and strategy*. Carlisle: Strategic Studies Institute, US Army War College, 2014. 198-210.

[7] Libicki, M. C. "The Convergence of Information Warfare". *Strategic Studies Quarterly* 11/1. 2017. 50.

use the same techniques (e.g. the subversion of computers, systems, networks). Second (2), the strategic aspects of these elements are converging (where on element of information warfare can be used, other elements might as well). Thirdly (3), some countries (e.g. Russia, China, Iran) are starting to combine information warfare elements.[8]

TERMINOLOGY

The seemingly ever faster evolution of human knowledge following the rapid development of new technologies results in appearance of new words and terms that reflect the new concepts created.[9] These new definitions matter because the underlying concepts can be perceived differently depending on the audience and the context used. In a closed environment, e.g. among colleagues during a discussion, the interlocutor may intuitively understand what their partners are trying to convey, or can directly ask for clarification. In a written context, or during a presentation, it is important to be precise because the reader or listener may come from a different background where the same term has another connotation.[10] To have clear and unambiguous communication among its members, NATO uses a standardized terminology (column 4 in the matrix table) to sustain its interoperability at all levels. For the purpose of this paper I looked into the terms related to psychological operations (PSYOPS), cyber operations (CYBEROPS), information operations (INFOOS), influence operations (INFLUENCEOPS) and information warfare (IW). For comparison to those definition were added the changing definitions used by the United States Department of Defense (US DoD)[11] and the Hungarian definitions of terms, with the similarities marked in bold.

Regarding the definition of psychological operations, common elements are as follows: it is a planned activity towards predominantly foreign audiences with the aim to influence. This is in line with one of the earlier definition of PSYOPS which was "the *planned use,* by a nation, of propaganda and related informational measures designed to *influence* the opinions, emotions, attitudes and behaviour of enemy, neutral or friendly *foreign groups* in such a way as to support the accomplishments of its national policy and aims". However the aim of influencing is different in the US, in the NATO and in Hungarian definitions, while the US PSYOPS focuses on the emotions, motives and objective reasoning of target groups, the NATO terminology works on the perceptions, attitudes and behaviours of these groups, the latter seeming a more nuanced and narrower approach to the hearts and minds of the audience.

Cyber operations (CYBEROPS) can either be offensive or defensive in theory, however only the US terminology adapted an offensive term. The latter is intended to project power through cyberspace, while the defensive CYBEROPS are generally to preserve freedom of action in cyberspace and to protect own data, networks and systems. The latter sentence of the US definition is more concrete than that of NATO, further narrowing the scope. The Hungarian National Security Strategy theoretically envisages the possibility of response in the physical space as well in the case of a serious cyber-attack.

---

8 Libicki. "The Convergence of Information Warfare". 52.

9 Georgieva, V. "Systematization of military terminology: mission (im)possible?". In *Foreign Language Competence as an Integral Component of a University Graduate Profile.* Brno: University of Defence, 2007. 86.

10 van Mil, J. W. F. and Henman, M. "Terminology, the importance of defining". *International Journal of Clinical Pharmacy* 38/3. 709-713. DOI: 10.1007/s11096-016-0294-5.

11 It should be noted that regarding the term 'PSYOPS' there is a difference of view between the US DoD and the US army.

Both PSYOPS and CYBEROPS are part of information operations (INFOOPS), which is a core function in all definitions examined here. While the US definition underlines its integrated nature, the NATO definitions elaborate it more (analyse, plan, assess and integrate), and while NATO's objective is to 'create the desired effect', the US definition's is to 'influence, disrupt, corrupt, or usurp' the adversaries' capabilities and preserve one's own. The US's definition is narrowing its scope to military operations, thus the inclusion of 'influence operations' (INFLUENCEOPS) in it. While it is not widely endorsed, its research was done by RAND Corporation, a think tank working with the US army. Influence operations might be the counterpart to 'peace time' operations, to the MISO (military information support operations). This differentiation is partly due to the fact that "in the US 90% of cyber activity is in private hands, thus the military should not be operating within 90% of the Internet unless it pertains to one of the mission sets." The U.S. Department of Defense used the term MISO instead between 2010–2017, after which they reverted to the term PSYOPS, understanding that MISO is part of what they do, but not who they are, and the change was primarily a terminological one.

Cyberspace is a force multiplier of INFOOPS activities as it can amplify a narrative, thus becoming more effective, e.g. confusing the target audience and diminishing its trust towards its government. Rand proposes as well the separation of INFOOPS into two parts: a technical function (with electronic warfare [EW] and computer network warfare [CNW], and an INFLUENCEOPS (including PSYOPS, operational security [OPSEC] and military deception [MILDEC]).

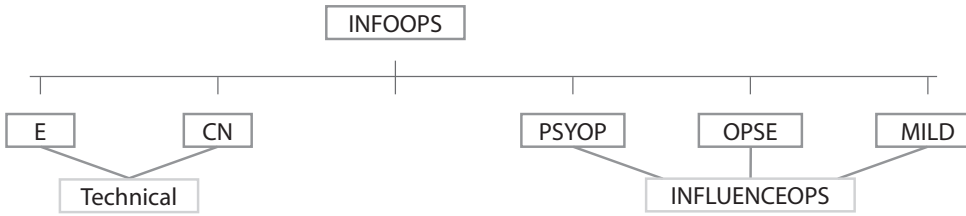

Figure 1 *The proposed classification by RAND*[12]

Although both INFOOPS and CYBEROPS can be used to achieve strategic information warfare goals, the efficiency of cyber operations as a medium for PSYOPS messages is inherent. An offensive cyberattack, e.g., the disruption of crucial webpage access, might have a psychological effect and influence decision makers, to change the behaviours of the target audience. An example of this is that during the COVID-19 crisis, DDoS (distributed denial of service) attacks increased in volume, targeting crucial infrastructure services like school and hospital websites. Kasperski's estimate is that the rates doubled in comparison to the final quarter of 2019, and surged by 80% year over year.[13] A further classification of INFOOPS is the overtness – covertness of it. INFOOPS can be overt (or white), which means that the sponsorship of the dissemination activity is known (source known and stated). Covert (black) information operations means that the ownership of such activity is denied or there is an attempt to have other source identified. The hybrid or grey area is when there is no attempt to either identify or conceal the source.[14]

[12] Porsche. *Redefining information warfare boundaries…* xxi.

[13] Kupreev, O., Badovskaya, E. and Gutnikov, A. "DDoS attacks in Q1 2020". *Kasperski Securelist*. 6 May 2020. https://securelist.com/ddos-attacks-in-q1-2020/96837/, Accessed on 10 June 2020.

[14] Smith. "Psychological Warfare". 46.

Table 1 *Matrix table*

Definitions	US DoD 1998 (U. S. Staff 1998)	US DoD 2006[I]
PSYOPS	Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.	No change. US DoD 2010 added: „in a manner favorable to the originator's objectives"
CYBEROPS	–	–
INFOOPS	"actions taken to affect adversary information and information systems, while defending one's own information and information systems" I-9	The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.
INFLUENCE OPS	–	–
INFORMATION WARFARE	"information operations conducted during time of crisis or conflict (including war) to achieve or promote specific objectives over a specific adversary or adversaries"[IX]	the Department of Defense removes the term "information warfare"

[I] "Joint publication 3-13: information operations". US Joint Chiefs of Staff. 13 February 2006. https://www.hsdl.org/?view&did=461648, Accessed on 7 May 2020.

[II] "Joint publication 3-12: cyberspace operations". US Joint Chiefs of Staff. 8 June 2018. https://www.hsdl.org/?view&did=812851, Accessed on 7 May 2020.

[III] *Ált/ 46: Lélektani műveletek doktrína.* Budapest: Magyar Honvédség, 2014. 13.

[IV] "1163/2020. (IV.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról". [Government Decree No. 1163/2020. on Hungary's National Security Strategy] *Magyar Közlöny* 81. 2020. 2101-2118.

[V] "Joint publication 3-13: information operations". US Joint Chiefs of Staff. 20 November 2014. https://www.hsdl.org/?view&did=759867

[VI] "NATO Standard AJP-3: Allied Joint Doctrine for the conduct of operations". NATO Standardization Office. February 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf

[VII] *Ált/57: Információs műveletek doktrína.* Budapest: Magyar Honvédség, 2014. 17.

[VIII] Made for the US army. Larson, E. V. et al. *Foundations of Effective Influence Operations: a Framework for En*hancing Army Capabilities. Santa Monica: RAND Corporation, 2009.

[IX] "Joint publication 3-13: joint doctrine for information operations". US Joint Chiefs of Staff. 9 October 1998. https://www.hsdl.org/?view&did=3759, Accessed on 7 May 2020. I-1.

[X] Theohary, C. A. "Defense Primer: Information Operations". Congressional Research Service. 14 January 2020. https://crsreports.congress.gov/product/pdf/IF/IF10771, Accessed on 8 May 2020.

US DoD 2018[II]	NATO (2019) AAP-06	HU
Use of „MISO": military information support operations.	Planned activities using methods of communication and other means directed at approved audiences in order to influence perceptions, attitudes and behaviour, affecting the achievement of political and military objectives.	Planned psyops activities using methods of communication and other means aimed at influencing the approved audiences' attitudes, behaviours and attitudes, thus affecting the achievement of political and military objectives.[III]
(Offensive) Missions intended to project power in and through cyberspace. (Defensive) Missions to preserve the ability to utilize cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating on-going or imminent malicious cyberspace activity.	Actions in or through cyberspace intended to preserve own and friendly freedom of action in cyberspace and/or to create effects to achieve military objectives.	N.B.: in the Hungarian National Security Strategy (2020) cyber capabilities capable of endangering physical security or causing significant material damage are considered weapons, and their use is considered armed aggression, to which a response in physical space is also possible.[IV]
The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own.[V]	A staff function to analyse, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences approved by the North Atlantic Council in support of Alliance mission objectives.[VI]	Staff function to analyse and plan the information environment. It plans, coordinates and assess the information activities, integrates them into the military capabilities in order to achieve the desired effect on the will, understanding and capability of the target audiences. Target audiences compromises of adversaries, potential adversaries and other politically approved audiences.[VII]
"application of national diplomatic, informational, military, economic, and other capabilities in peacetime, crisis, conflict, and post-conflict to foster attitudes, behaviours, or decisions by foreign target audiences that further U.S. interests and objectives"[VIII]	–	–
"While there is currently no official U.S. government (USG) definition of information warfare (IW), practitioners typically conceptualize it as a strategy for the use and management of information to pursue a competitive advantage, including both offensive and defensive operations."[X]	–	–

Some countries (e.g. Russia, China, Iran) are starting to combine INFOOPS elements. "The *hearts and minds* is a principal centre of gravity in operational and tactical planning and execution. This insistence on regarding psychological warfare as central to the conduct of war stands in contrast to the role of psychological warfare in major Western military establishments, where it is generally seen as supplemental and of secondary importance"[15]. These countries are integrating and deploying cyberspace and psychological capabilities in ways consistent with their doctrine, strategy, organizational culture, and risk tolerance. The use of new capabilities evolve as they are introduced in conflicts, and thus brings a maturation of operational concepts and strategic insights[16]. A brief example of this is the fact that the Russians generally do not use the terms cyber or cyberwarfare, except when referring to foreign writings on the topic. "They tend to use the word *informatization,* which is a holistic concept that includes computer network operations, electronic warfare,

[15] "Psychological warfare". *Encyclopedia Brittania*. https://www.britannica.com/topic/psychological-warfare, Accessed on 10 June 2020.

[16] Nakasone, P. M. "A cyber force for persistent operations". *Joint Force Quarterly* 92/1. 2019. 12.

psychological operations, and information operations. In other words, cyber is regarded as a mechanism for enabling the state to dominate the information landscape, which is regarded as a warfare domain in its own right."[17]

Russia has also developed capabilities for Information Warfare which includes Computer Network Operations, Electronic Warfare, Psychological Operations, and Deception activities.[18] Russia views information warfare as a soft power tool to be used both in peacetime and wartime. Indeed, it is an ongoing activity regardless of the state of relations with the opponent; in contrast to other forms and methods of opposition, information confrontation is waged constantly in peacetime.[19] (p.4.) As per the Russian concepts, Information Warfare in the new age conditions will be the starting point of every action now called the new type of warfare, or hybrid war, in which broad use will be made of the mass media and, where feasible, global computer networks (blogs, various social networks, and other resources)[20] It is also a point of view, that "Russia faces fewer legal and cultural barriers to influence at the operational and strategic level and it also has philosophically different approaches and goals while operating in the information environment".[21] This difference can be seen in the definition presented, whereas IW is an "intensive struggle in the information environment with the aim of achieving informational, psychological and ideological superiority, damaging information infrastructure, undermining political and social systems, as well as psychologically shaping military personnel and populations".[22] Bruce Schneier presents 8 steps that are frequently used in influence operations, and to which he proposes countermeasures as well. In his view, the following happens in a successful campaign: (1) exploit societal division and weaken trust in government, (2) build audience, (3) create distortion through alternative narratives, (4) have some truth to those narratives, (5) conceal (attribution), (6) amplify narratives, (7) deny involvement and (8) focus on long-term impact.[23] These steps show resemblance to the disinformation campaigns and narratives, which is often taken under the umbrella of information operations.[24]

Some other risks include big data and artificial intelligence. As humans become more connected via different devices, their production of personal data increases. These data, including health, purchases, and GPS tracking, can describe individuals to a high level of detail. If there is access to these data from legitimate (or illegitimate) data brokers, matching these different types of data can be a goldmine for precision targeting and microtargeting. Thus, it has become easier for covert or grey information warfare to target key figures with the intended messages. On the other hand, with the data and information at hand, the creation of 'shallowfakes' (manually alter images), 'deepfakes' (the use of artificial intelligence

---

17 Connell, M. and Vogler, S. *Russia's approach to cyber warfare*. Arlington, VA: Center for Naval Analysis, 2017. 3.

18 Ajir, M. and Vailliant, B. "Russian Information Warfare : Implications for Deterrence Policy". *Strategic Studies Quarterly* 12/3. 2018. 74.

19 Giles, K. *Handbook of Russian Information Warfare.* Rome: NATO Defense College, 2016. 4.

20 Giles. *Handbook of Russian Information Warfare.* 6.

21 Tashev, B., Purcell, M. and McLaughlin, B. "Russia's Information Warfare, Exploring the Cognitive Dimension". *Marine Corps University Journal* 10/2. 2019. 132. DOI: 10.21140/mcuj.2019100208.

22 Tashev, Purcell and McLaughlin. "Russia's Information Warfare…" 136.

23 Schneier, B. "8 ways to stay ahead of influence operations". Foreign Policy, 12 August 2019. https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/, Accessed on 15 May 2020.

24 Weitz, R. "Assessing the Russian Disinformation Campaign During COVID-19". International Centre for Defence and Security. 13 November 2020. https://icds.ee/en/assessing-the-russian-disinformation-campaign-during-covid-19/, Accessed on 20 December 2020.

to manipulate or generate visual and audio content with a high potential to deceive) and 'social bots' (an agent that communicates more or less autonomously on social media, often with the task of influencing the course of discussion and/or the opinions of its readers,[25] will also become more realistic.

On the other hand, in the case of the United States, its legal and doctrinal scope is narrower. The "DoD has three primary cyber missions: (1) defend DoD networks, systems and information, (2) defend the US homeland and US national interests against cyberattacks of significant consequence and (3) provide cyber support to military operational and contingency plans. There is pressure on DoD to participate in cyber operations outside their three stated mission sets. The military operates in four areas of the cyberspace: intelligence, information, crime and military operations."[26] A change in the doctrine would mean of course that if "the US CYBEROPS became part of a broader understanding of IW, US Cyber Command would have to broaden its mission as well"[27].

As we have seen thus far, CYBEROPS and PSYOPS are usually classified beneath INFOOPS, as part of it. An interesting proposition by Ajir and Vaillant takes another approach, and proposes the integration of INFOOPS separately under CYBEROPS and PSYOPS: the cyber domain (virtual) and a psychological domain (cognitive)[28] by the effects of information operations on the target. The writers underline this step from the lenses of deterrence (and classical deterrence theory) and while the idea has merit during my research I have not found other sources in favour of such changes.

An interesting point made by Smith is that defence against the enemy's psychological operations is limited responsibility of one's own PSYOPS. This is partly because the "target is not the opposing PSYOPS forces as in normal warfare, and the 'minds' include neutral and friendly foreign groups as well."[29] This opinion seems to converge with other elements, notably that "the current information warfare domain is 'offence-dominant' – it is easier to create malign content and apps than it is for governments and social media platforms to identify and counter these threats"[30].

CONCLUSION

The aim of this article was to give an overview of the terminology used regarding psychological operations and how it has changed as the intent and tools used for its purpose evolved. Three essential points should be made regarding the discussed topic. First, it would be important to clearly define the content, roles and methods of the operation types (PSYOPS, INFOOPS, CYBEROPS) to avoid the duplication of frameworks used, while keeping in mind a pragmatic and horizontal approach. Secondly, derived from this mainstreamed approach, the changes in the organizational structure should follow – not only at command level, but also at personnel level. Thirdly, a better understanding and consideration should be given to the different approach ('grey zone') to influence by other parties. It should also be noted, that there is a third area that interlaps with both PSYOPS and CYPEROPS, and that is disinformation.

---

25 Ferrara, E. et al. "The Rise of Social Bots". *Communications of the ACM* 59/7. 2016. 96-104. DOI: 10.1145/2818717.

26 Crowther. "The Cyber Domain". 64-65.

27 Libicki. "The Convergence of Information Warfare". 61.

28 Ajir and Vaillant. "Russian information warfare…". 86.

29 Smith. "Psychological Warfare". 41.

30 Weitz. "Assessing the Russian Disinformation Campaign During COVID-19".

This article has very lightly touched upon it, and INFLUENCEOPS or grey area PSYOPS might cover some of its elements, it still poses a difficulty to categorize disinformation operations neatly. It is possible that a new, encompassing term will emerge, or that over time one of the terms will become more prominent. At this point what can be seen is that some allied countries (e.g. the Czech Republic, Germany, Poland, Sweden) are upgrading their structures reflecting the changed importance of information operations, including PSYOPS and CYBEROPS. As it is important to take into account the context and cultural, theoretical background when discussing terms and definitions, so it is regarding what constitutes cyber operations and psychological operations in the transatlantic and in other military cultural context, as it would bring clarity as to what are we seeing today. Just as conventional warfare has changed in the last decades, and unconventional warfare has become more prominent, so is the digital (cyber) landscape changing, with multiple different actors and intents present, and thus creating a (cyber)fog of war.

BIBLIOGRAPHY

"1163/2020. (IV.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról". [Government Decree No. 1163/2020. on Hungary's National Security Strategy] *Magyar Közlöny* 81. 2020. 2101-2118.

Ajir, M. and Vailliant, B. "Russian Information Warfare: Implications for Deterrence Policy". *Strategic Studies Quarterly* 12/3. 2018. 70-89.

Ált/46: Lélektani műveletek doktrína. Budapest: Magyar Honvédség, 2014.

Ált/57: Információs műveletek doktrína. Budapest: Magyar Honvédség, 2014.

Connell, M. and Vogler, S. *Russia's approach to cyber warfare.* Arlington, VA: Center for Naval Analysis "The Cyber Domain". *The Cyber Defense Review* 2/3. 2017. 63-78.

Daugherty, W. E. "Origin of Psyop Terminology". In Mclaurin, R. D. (ed.) *Military Propaganda: Psychological Warfare and Operations.* New York: Praeger Publishers, 1987. 255-271.

Ferrara, E., Varol, O., Davis, C., Menczer, F. and Flammini, A. "The Rise of Social Bots". *Communications of the ACM* 59/7. 2016. 96-104. DOI: 10.1145/2818717

Georgieva, V. "Systematization of military terminology: mission (im)possible?". In *Foreign Language Competence as an Integral Component of a University Graduate Profile.* Brno: University of Defence, 2007. 85-104.

Giles, K. *Handbook of Russian Information Warfare.* Rome: NATO Defense College, 2016.

Haig, Zs., and Várhegyi, I. "A cybertér és a cyberhadviselés értelmezése". *Hadtudomány* 18/e. 2008. 1-12. http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf

"Joint publication 3-12: cyberspace operations". US Joint Chiefs of Staff. 8 June 2018. https://www.hsdl.org/?view&did=812851, Accessed on 7 May 2020.

"Joint publication 3-13: information operations". US Joint Chiefs of Staff. 13 February 2006. https://www.hsdl.org/?view&did=461648, Accessed on 7 May 2020.

"Joint publication 3-13: joint doctrine for information operations". US Joint Chiefs of Staff. 9 October 1998. https://www.hsdl.org/?view&did=3759, Accessed on 7 May 2020.

"Joint publication 3-13: information operations". US Joint Chiefs of Staff. 20 November 2014. https://www.hsdl.org/?view&did=759867

Jones, F. L. "Information: the psychological instrument". In Bartholomees, J. B. (ed.), U.S. *Army War College guide to national security policy and strategy.* Carlisle: Strategic Studies Institute, US Army War College, 2014. 198-210.

Kupreev, O., Badovskaya, E. and Gutnikov, A. "DDoS attacks in Q1 2020". *Kasperski Securelist.* 6 May 2020. https://securelist.com/ddos-attacks-in-q1-2020/96837/, Accessed on 10 June 2020.

Larson, E. V., Darilek, R. E., Gibran, D., Nichiporuk, B., Richardson, A., Schwartz, L. H. and Thurston, C. Q. *Foundations of Effective Influence Operations: a Framework for Enhancing Army Capabilities.* Santa Monica: RAND Corporation, 2009.

Libicki, M. C. "The Convergence of Information Warfare". *Strategic Studies Quarterly* 11/1. 2017. 49-65.

Myers, M. "The Army's psychological operations community is getting its name back". *Army Times,* 6 November 2017. https://www.armytimes.com/news/your-army/2017/11/06/the-armys-psychological-operations-community-is-getting-its-name-back/, Accessed on 30 November 2020.

Nakasone, P. M. "A cyber force for persistent operations". *Joint Force Quarterly* 92/1. 2019. 10-14.

"NATO Standard AJP-3: Allied Joint Doctrine for the conduct of operations". NATO Standardization Office. February 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf

Porsche III, I. R., Paul, C., York, M. , Serena, C. C., Sollinger, J. M., Axelband, E., Min, E. Y. and Held, B. J. *Redefining information warfare boundaries for an army in a wireless world.* Santa Monica: RAND Corporation, 2013.

Post, J. M. "The key role of psychological operations in countering terrorism". In Forrest, J. J. F. (ed.) *Countering Terrorism and Insurgency in the 21st Century: Strategic and Tactical Considerations.* Westport: Praeger Security International, 2007. 380-392.

„Psychological warfare". Encyclopedia Brittania. https://www.britannica.com/topic/psychological-warfare, Accessed on 10 June 2020.

Schneier, B. "8 ways to stay ahead of influence operations". Foreign Policy, 12 August 2019. https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/, Accessed on 15 May 2020.

Smith, C. H. "Psychological Warfare". *Naval War College Review* 6/2. 1953. 39-61.

Theohary, C. A. "Defense Primer: Information Operations". Congressional Research Service. 14 January 2020. https://crsreports.congress.gov/product/pdf/IF/IF10771, Accessed on 8 May 2020.

van Mil, J. W. F. and Henman, M. "Terminology, the importance of defining". *International Journal of Clinical Pharmacy* 38/3. 709-713. DOI: 10.1007/s11096-016-0294-5.

Weitz, R. "Assessing the Russian Disinformation Campaign During COVID-19". International Centre for Defence and Security. 13 November 2020. https://icds.ee/en/assessing-the-russian-disinformation-campaign-during-covid-19/, Accessed on 20 December 2020.

Tashev, B., Purcell, M. and McLaughlin, B. "Russia's Information Warfare, Exploring the Cognitive Dimension". *Marine Corps University Journal* 10/2. 2019. 129-147. DOI: 10.21140/mcuj.2019100208.