Volume 6 Issue 4 2019

Journal of Corporate Responsibility
and Leadership

Leadership and Human Behaviours in the Context
of Information and Knowledge Management

The Perception of Information and Its Role in Exercising Military Leadership

doi: http://dx.doi.org/10.12775/JCRL.2019.013

Tomasz Kacała
Joint Force Training Centre, Bydgoszcz, Poland
e-mail: tomasz1975@yahoo.com

Abstract

Purpose: The main purpose of the research was to investigate the way the information is perceived and the role it plays in exercising military leadership, especially in the context of differences between the Allied interpretations of the term and the Russian concept of *information* as an instrument of military strategy. The aim of the paper was to find out, indicate and describe the role and perception of information in different areas of military interest, both within the Alliance and outside of this. Operationalizing the aforementioned aim the following research questions have been set: what are the differences in definitions of information? what are the objectives and principles applied in various kinds of military, information-related activities? what is the role of information in exercising leadership?

Design/methodology/approach: Research methodology examined from the perspective of its objectives, in this case, can be classified as descriptive (describing systematically the perception of information, providing required input of expertise and attitudes towards the role of information) and explanatory (clarifying the differences in understanding the concept of information, e.g. in operations and management). If one considers the perspective of 'mode of enquiry', the qualitative approach (aiming at exploring diversity rather than quantifying and emphasizing the description of perceptions rather than their measurement) has been applied here. The basic part of research, for the purpose of the paper

development, was literature (doctrinal documents) review as well as subject matter (Russian information-related capabilities and activities) summaries collation.
Findings: The research shows that the perceptions of information presented by the Alliance and the Russian Federation differ substantially. The roles played by information in exercising military leadership vary as well. Considering Russian perception of information, its main concept is included in the fundamentals of *information confrontation* as a form of warfare. The Allied interpretation of the term focuses on data, intelligence and knowledge represented in many diverse forms.
Research and practical limitations/implications: The research conduct and its scope were limited by two factors: availability of the most updated doctrinal documents (the Alliance) and access to original sources (Russia). The NATO doctrinal documents, to include policies and allied joint publications, are often subject to a long term revision process and thus may not be up to date in many aspects included in their contents. Whereas, the Russian sources are often classified or characterized by limited accessibility.
Originality/value: The differences in the information perception have not been compared in such a set yet, especially internally within the Alliance – Information/Knowledge Management and Information Operations. Moreover, the wider context of Russian understanding of the apparatus applied within the Information Environment, though identified, have not been collated with the Allied approach either.
Paper type: research paper.

Keywords: information, propaganda, disinformation, misinformation, post-truth, fake news, trolls, bots, hacktivists.

1. Introduction

These days are often described as the ‘Information Age’ due to the fact that *information* has become a paramount factor affecting literally every aspect of our lives. Information has become the meaning of itself, the value of its own. This is the reason why it plays a very important role in each and every dimension of our realm, including social, political, economic and military one. The interpretations of the term itself may vary as there are lots of points of view on the ‘information’. It depends on the perspective one applies. The military tends to lean toward the idea of warfare or operation – as the result we can find the Allied concept of Information Operations (INFO OPS) – whereas the civilian community is more likely to prefer the term ‘management’ – Information

Management – that quite often transfers into another extended category of Information and Knowledge Management (IKM). It is important to remember that the two concepts are not contrary but different, do not exclude each other but complement. What is more, some manifestations of the knowledge management concept institutionalization are observed within the Alliance (Lis 2014; 2015).

Proper understanding of the diversified interpretations of the term requires a thorough analysis of respective fundamentals – definitions, objectives and principles, roles and responsibilities. All of them have been included in the respective publications released by the Alliance within the last few years' period. Therefore, the main purpose of the research is to investigate the way the information is perceived and the role it plays in exercising military leadership, especially in the context of differences between the Allied interpretations of the term and the Russian concept of *information* as an instrument of military strategy. The aim of the paper is to find out, indicate and describe the role and perception of information in different areas of military interest, both within the Alliance and outside of this. Operationalizing the aforementioned aim the following research questions have been set: what are the differences in definitions of information? what are the objectives and principles applied in various kinds of military, information-related activities? what is the role of information in exercising leadership?

The applied research methodology examined from the perspective of its objectives, in this case, can be classified as descriptive (describing systematically the perception of information, providing required input of expertise and attitudes towards the role of information) and explanatory (clarifying the differences in understanding the concept of information, e.g. in operations and management). If one considers the perspective of 'mode of enquiry', the qualitative approach (aiming at exploring diversity rather than quantifying and emphasizing the description of perceptions rather than their measurement) has been applied here. The basic part of research, for the purpose of the paper development, was literature (doctrinal documents) review as well as subject matter (Russian information-related capabilities and activities) summaries collation.

The research conduct and its scope were limited by two factors: availability of the most updated doctrinal documents (the Alliance) and access to original sources (Russia). The NATO doctrinal documents, to include policies and allied joint publications, are often subject to a long term revision process and thus may not be up to date in many aspects included in their contents. Whereas, the Russian sources are often classified or characterized by limited accessibility.

2. Definitions

The analysis and comparison of INFO OPS and IKM interpretations should definitely begin with the identification of the ultimate assumption – definition of the term ‘information’. In order to properly understand other concepts of information utilisation, such as Russian perception of modern, political and military, activities undertaken in the multinational environment, it seems to be advisable to introduce the interpretations of such terms as information confrontation, disinformation, misinformation, propaganda, post-truth or fake news.

The Alliance functions utilizing the same scope of applied definitions – this is the ultimate condition, prerequisite of its interoperability. Therefore, one of its agencies, NATO Standardization Office (NSO), updates and regularly releases *AAP-6 NATO Glossary of Terms and Definitions*. Its latest edition (2018) describes information as “unprocessed data of every description which may be used in the production of intelligence” (AAP-6, 2018, p. 65). The same definition has been used in *AJP-3.10 Allied Joint Doctrine for Information Operations*. As far as one considers the IKM-related documents, the definition is different. According to the documents (NATO Information Management Policy/NIMP, 2007, p. 1–4; Primary Directive on Information Management/PDIM, 2008, p. 1-C-1) information is “any communications or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audio-visual forms”. It may result from the fact that the two fundamental publications – Policy and Directive – were released respectively in 2007 and 2008. One point needs to be noted here – NATO (Bi-Strategic Commands: Allied Command Operations and Allied Command Transformation) IKM Policy and Directive are being currently reviewed and will be updated and released in the future.

The term *information operations* is defined as “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 North Atlantic Council (NAC) approved audiences in support of Alliance mission objectives" (MC 0422/5 NATO Military Policy for Information Operations, 2015, p. 4) and will be proposed for inclusion in *AAP-6*. NAC approved audiences also require explanation – they are "those identified in top-level political guidance on Alliance information activities. These may include adversaries, potential adversaries, decision-makers, cultural groups, elements of the international community and others who may be engaged by Alliance information activities" (AJP-3.10 Allied Joint Doctrine for Information Operations, 2015, p. 1–5).

The definition of *information management* provided by IKM-related documents describes this activity as "a discipline that directs and supports the handling of information throughout its life-cycle ensuring it becomes the right information in the right form and of adequate quality to satisfy the demands of an organisation" (NIMP, 2007, p. 1–4; PDIM, 2008, p. 1-C--2). The difference between a staff function and a discipline seems to be the indication of mind-set diversity – operation-oriented on the one hand and scientifically driven (management-related) on the other.

Information confrontation or IPb (informatsionnoye protivoborstvo) is "the Russian government's term for conflict in the information sphere. IPb includes diplomatic, economic, military, political, cultural, social and religious information arenas, and encompasses two measures for influence: informational-technical effect and informational-psychological effect. Informational-technical effect is roughly analogous to computer network operations, including computer network defence, attack, and exploitation. Informational-psychological effect refers to attempts to change people's behaviour or beliefs in favour of Russian governmental objectives" (DIA, 2017, p. 38).

Thus, the Russian concept of *information* relates to "an instrument, a target, and an operational space in which confrontation unfolds" (Averin, 2018, p. 62). "This information can be stored anywhere, and transmitted by any means – so information in print media, or on television, or in somebody's head, is subject to the same targeting concepts as that held on an adversary's computer or smartphone. Similarly, the transmission or transfer of this information can be by any means: so introducing corrupted data into a computer across a network or from a flash drive is conceptually no different from placing disinformation in a media outlet, or causing it to be repeated in public by a key influencer" (Giles, 2016, p. 10).

Propaganda has a number of definitions and interpretations. For the purpose of this article it will be described as a kind of activity that "does not disregard truth, but uses elements of truth in the deliberate, systematic attempt to shape perceptions in order to achieve a specific response or reaction from an audience, meant to benefit and further the desired intent of the propagandist" (Jowett and O'Donnell, 2015, p. 7, 15).

The term *disinformation* is "the manipulation of information that purposefully aims to mislead and deceive, while misinformation is inaccurate information that is the result of an honest mistake or of negligence" (Fallis, 2015, pp. 401–402).

Post-truth, especially being a part of the phrase *post-truth politics*, is defined as "a situation where appeals to emotion are dominant and factual rebuttals or fact checks are ignored on the basis that they are mere assertions". The most important element seems to be "the ability […] to appeal to the instincts and nostalgic emotions of a group" (Suiter, 2016, pp. 25, 27).

And the definition of *fake news* includes "dissemination of false information via media channels (print, broadcast, online). This can be deliberate (disinformation), but can also be the result of an honest mistake or negligence" (McManus and Michaud, 2018, p. 19).

3. Objectives and principles

As it was stated in the definition cited above, the main objective of INFO OPS is "to create desired effects on the will, understanding and capability of selected target audiences" (AJP 3–10, 2015, p. 1–5). More detailed, implied objectives, however, have been encompassed by the interrelated areas INFO OPS comprises. They include: "preserving and protecting Alliance freedom of action in the information environment at all times; shaping behaviours, perceptions and attitudes of NAC approved audiences and countering an adversary's propaganda as well as their command and control (C2) functions and capabilities" (AJP 3–10, 2015, p. 1–6). One can identify here three main groups of actors involved: own decision-makers, NAC approved audiences and adversary's C2 elements. Own decision-makers and the processes they take part in defending the related data, networks and information. Considering NAC approved audiences, they need to be induced, reinforced, convinced or encouraged to support Alliance military operations and achievement of NATO objectives. Whereas, adversary's opinion forming and decision-making processes should be countered. The INFO OPS objectives, though not explicitly expressed, include the component of affecting adversary's functions and capabilities. The IKM-related documents present a much stronger view on this matter.

Both Policy and Directive clearly specify the three key objectives of Information Management. They include: "to support the achievement of Information Superiority primarily within an information sharing networked environment, to support the effective and efficient use of information resources in the conduct of the NATO mission, and to support the identification and preservation of information of permanent value to NATO" (NIMP, 2007, p. 1–1; PDIM, 2008, p. 1–6). What draws attention here is the term *Information Superiority* defined as "a state of relative advantage in the information domain achieved by getting the right information to the right people at the right time in the right form whilst denying an adversary the ability to do the same" (NIMP, 2007, p. 1–5). The term does not occur in Directive or the latest edition of AAP6, which may be the confirmation of a certain phenomenon that has been observed lately in this area. The phenomenon consists in *softening* the previously applied concept of *information warfare* and replacing it with currently exercised INFO OPS (Modrzejewski, 2015, pp. 14–15). Further differences between INFO OPS and IKM may also be identified in terms of the principles applied.

In order to properly plan and conduct information activities, certain principles have been developed and established. They are based on the assumption that one needs to understand the commander's objectives, guidance, intent and the overall situation in the information environment. It will enable shaping the appropriate role of INFO OPS within several processes including planning and targeting. The principles characterize and determine INFO OPS as: focused and integrated, coherent, consistent, and continuous. Moreover, there are a few ideas that should be considered as well. They encompass comprehensive understanding, centralized planning and decentralized execution, monitoring, assessment and agility (AJP 3–10, 2015, pp. 1–8 – 1–10). Information Operations should focus on the effects necessary to achieve the commander's objectives and then choose the most suitable sort of activity to generate the effect. All the involved elements such as words, images and actions need to be coherent with one another on every level (tactical, operational and strategic). A very relevant condition of a successfully conducted operation is a thorough understanding of the environment, most particularly, the human terrain defined as “the social, political and economic organization, beliefs and values, and forms of interaction of a population” (AJP 3--10, 2015, p. 1–9). INFO OPS need to be fully integrated in the overall preparation and conduct effort so commanders should be prepared to delegate authority to lower levels of C2 structure. Although, there may be situations where centralized execution of tasks will be required. Continuous monitoring and assessment of the short and long-term effects is a key part of effective INFO OPS. Measures of Performance (MOP) and Measures of Effectiveness (MOE) are the two most significant ways of the monitoring and assessment implementation. The latter is, according to the INFO OPS doctrine, a prerequisite of Knowledge Development (KD) process consisting in rendering the meaning from data and information by the use of the skills acquired through experience or education in order to contribute to the theoretical or practical understanding of a subject (AJP 3–10, 2015, p. 1–10). And last but not least, agility is required from INFO OPS in order to adequately respond to constantly changing conditions of the operational and information environment.

The principles applied by Information and Knowledge Management seem to be much more information-oriented. They include: perception of *information* as a corporate resource, information ownership and custodianship, leadership and organisational structure, information sharing, information standardisation, information assurance and information needs (NIMP, 2007, pp. 1–1 – 1–1; PDIM, 2008, pp. 1–6 – 1–7). The corporate nature of information provides support for NATO’s missions, consultation, decision-making processes, and operational requirements. It is achieved by organising and controlling information throughout its lifecycle regardless of the medium and format in which it is held. Information requires a number of its life-cycle participants to include an originator, an owner and a custodian. Involvement of leadership and use of an effective organisational structure are parts of responsibility related to information management. One of the most important IKM principles is the one of ‘need-to-know’. It is directly connected with the responsibility to share information with other stakeholders – participants and members of IKM community.

Achievement and maintaining of information standards is a key prerequisite of effective and efficient interoperability. Security of information, also known as information assurance, includes a set of measures required to achieve a given level of confidence and protection. Intended activities and effects may be met by implementation of planning and architecture processes that are defined as “the activities of designing and maintaining a representation (i.e. blueprint) of components of a business (i.e. organisation, processes, information, technology) and their relationships in order to understand where, when and why information is required” (NIMP, 2007, p. 1–2; PDIM, 2008, p. 1–7).

There are opinions that “recently published Russian military theory gives *information warfare* an increasingly prominent role. Recognition that Russia cannot compete directly in conventional terms with NATO has led to persistent emphasis in public statements on finding asymmetric responses. Information warfare is presented as one of these responses, and specifically as a means of assuring victory in armed conflict by predetermining the outcome. In its more ambitious descriptions, information warfare is considered capable of avoiding the necessity of armed conflict altogether by achieving strategic goals on its own” (Giles, 2016, p. 16). According to some analysts, Russia is showing “willingness to give primacy to non--kinetic operations, especially information warfare. The traditional [Western] assumption has been that subversion, deception, and the like are ‘force multipliers’ to the combat arms, not forces in their own right. At present, though, Russia is clearly seeing the kinetic and non--kinetic as interchangeable and mutually supporting” (Galeotti, 2016, p. 291).

The objectives and aims of the Russian information warfare campaigns can be both offensive and defensive. Wide categories of the above mentioned items include: strategic victory, reflexive control, permissive environment, subversion and destabilisation, and defensive measures (Giles, 2016, pp. 17–30). Considering strategic victory, Russian publications on military theory mention that “under today’s conditions, means of information influence have reached a level of development such that they are capable of resolving strategic tasks” (Chekinov and Bogdanov, 2011, pp. 3–13). Moreover, it is believed that “winning information confrontations will result in the achievement of strategic and political goals and in the defeat of an enemy’s armed forces and the capture of his territory, destruction of his economic potential, and overthrow of his political system” (Slipchenko, 2013, p. 52). At the same time it is worth noticing that, according to certain predictions, “involvement of conventional military forces is reduced to a minimum, and they are replaced by effective use of the Internet” (Giles, 2016, p. 18). Information-related effects – to include the application of the Internet for shaping consciousness of the masses – can, in certain situations, provide a substitute for armed intervention (Kartapolov, 2015, pp. 28–29).

Reflexive control is the concept consisting in “predetermining an adversary’s decision in Russia’s favour, by altering key factors in the adversary’s perception of the world. As such, it represents a key asymmetric enabler to gain critical advantages, neutralising the adversary’s strengths by causing him to choose the actions most advantageous to Russian objectives” (Snegovaya, 2015, p. 9). Public discussion in Russia shows a tendency to replace the term with ‘perception management’ having a meaning similar to the Western way of interpreting it. This category of information campaign does not need to be limited to influencing a single decision. Reflexive control means to induce the adversary to make a number of decisions that successively turn down options that would enhance their situation, until they are eventually “faced with a choice between bad and worse, either of which options would favour Russia” (Giles, 2016, p. 20).

Permissive environment is related to the Russian influence on foreign decision-makers. The influence is achieved by providing polluted information, taking advantage of the fact that Western political representatives receive the same information as their electing voters. Disinformation disseminated in this way constitutes a part of the decision framework creating chances for Moscow’s success. The reason for such a situation is a key element of reflexive control that is then in place. Even if this sort of activity is not successfully implemented, and only occurs in mass and social media, the outcome can be to form a permissive public opinion environment where a Russian way of presenting narratives, as well as their content, is perceived as factual. This level of influence provides Moscow with a possible gain, which is “to win public support in adversary nations, and thereby attenuate resistance to actions planned by Russia, in order to increase their chances of success and reduce the likelihood of damaging adverse reactions by the international community” (Giles, 2016, p. 22).

Subversion and destabilisation seem to be located at the lower end of the scale of information warfare ambition. The fundamentals of activities like this, and some of their guiding principles, may be broadly recognizable as “reinvigorated aspects of subversion campaigns from the Cold War era and earlier” (Madeira, 2014). The campaigns of that kind, and especially their certain aspects, were referred to as ‘active measures’ in the Soviet terminology of the time. Major Finnish study describes active measures as constituting “certain overt and covert techniques for influencing events and behaviour in, and actions of, foreign countries. [They] may entail the following objectives: influencing the policies of another government, undermining confidence in its leaders and institutions, disrupting the relations between other nations, discrediting and weakening governmental and nongovernmental opponents” (Pynnoniemi and Racz, 2016, p. 38).

And last but not least, defensive measures that result from awareness of the destructive capabilities of the techniques outlined already. It is related to the fact that Russia seems to be very successful in re-establishment of control over the information disseminated amongst its own population. For Russian decision-makers, this is a part of “implementing the requirements of its information security doctrine of ‘securing national information space’, and protecting it against ‘breaches’. Both of these isolationist concepts are unfamiliar for the West, but were traditional security preoccupations for Russia both during and before Soviet times” (Giles, 2016, p. 27). Possibility of owning media outlets by foreign enterprises has been limited, licenses for rebroadcasting suspended, and independent sources of news closed or constrained (Tsvetkova and Devitt, 2016). There is one element repeating itself in this process: acquisition of commercial control over media companies by Kremlin-friendly individuals, directly or indirectly influencing the editorial approach later on. Russian free media remains have been either marginalised or forced to cooperate with the government. There have been many cases of mainstream journalists reverting “to its former role of transporting leadership messages into the public space” (Giles, 2016, p. 28).

The objectives listed above can be achieved by the implementation of information confrontation means and actions that, according to the Russian theoreticians and practitioners, should follow certain principles. They include: “direct lies for the purpose of disinformation both of the domestic population and foreign societies; concealing critically important information; burying valuable information in a mass of information dross; simplification, confirmation and repetition (inculcation); terminological substitution – use of concepts and terms whose meaning is unclear or has undergone qualitative change, which makes it harder to form a true picture of events; introducing taboos on specific forms of information or categories of news; image recognition – known politicians or celebrities can take part in political actions to order, thus exerting influence on the world view of their followers; providing negative information, which is more readily accepted by the audience than positive" (Kuleshov, 2014, p. 107).

Russian subversion and weakening follow certain principles to include "targeting a broad range of areas which the West does not traditionally think of as vulnerabilities", for instance, "political, economic, information, scientific-and-technical, moral, culturological, demographic and environmental potentials" (Giles, 2016, p. 48). A very interesting and unique term 'culturological warfare' means "coercive action or counteraction with regressive or progressive goals in the sphere of science, education, pastoral care, the arts, the national language, religion and traditional ways of life" (Kvachkov, 2004).

4. Roles and responsibilities

NATO Military Policy for Information Operations distinguishes three main levels of responsibility as far as INFO OPS are concerned: Military Committee (MC), Strategic Commands (SC) and Nations (MC 0422/5, 2015, pp. 8–10). The responsibility of MC for NATO INFO OPS is exercised through International Military Staff (IMS) – Operations Division. There is even a specialized body established – MC Working Group (Operations) in the INFO OPS format. The specific MC responsibilities in this regard include: provision of INFO OPS related military advice to NAC; maintenance of an effective INFO OPS policy; provision of military guidance for INFO OPS and promulgation, monitoring, coordination and contribution to development of the INFO OPS doctrine. Moreover, MC is responsible for: development of INFO OPS related Crisis Response Measures (CRM), directing SC as required, adjustment to NATO INFO OPS guidance to reinforce NATO goals and provision of the Strategic Communication (StratCom) guidance. The responsibilities of SC are as follows: consideration of INFO OPS resource requirements, effects and audiences; integration of INFO OPS analysis and assessments into the planning process; integration of INFO OPS doctrine/plans at the strategic level and development and/or improvement of capabilities, techniques and security guidance. Additionally, SC are responsible, *inter alia*, for integration of INFO OPS into existing and future operational planning documents; review and request for approval of INFO OPS related CRM; development of training standards and integration of INFO OPS into training, exercises and evaluations in representative environments. As far as Nations are concerned, their responsibilities encompass: consideration of Alliance INFO OPS requirements during the NATO defence planning process and implementation of these requirements as appropriate into national planning; development of INFO OPS procedures within the framework of this document; provision of adequate intelligence in order to support NATO INFO OPS; inclusion of INFO OPS in training and exercises; and provision of resources and trained personnel to source NATO requirements and execution of NATO INFO OPS in operations and exercises.

The scope of roles and responsibilities defined by NATO Information Management Policy differs significantly (NIMP, 2007, pp. 1–2 – 1–3). The approach presented here seems to be more of a 'bottom-up' nature as its considerations begin with "individuals who produce or have authorized access to information to follow the principles of information management, originators and information owners" (NIMP, 2007, p. 1–2). Their responsibility includes: setting the rules for handling the information throughout its life-cycle and establishment of the rules for the transfer of ownership. The next category of entities – information custodians – is responsible for management and provision of the information under their custodianship following the rules set by the information owners. The heads of NATO and military bodies are required to ensure the compliance with Policy and other relevant (related) documents; to ensure the continuity of key services and operations by identification and protection of essential information; and to make sure that the disposition of information is conducted in accordance with established policies and procedures. Furthermore, the individuals are responsible for assessment of management effectiveness and efficiency; implementation of organisational, governance and accountability structures, as well as training programmes, for information management; and appointment of senior IM officials. National Authorities need to ensure that Policy and other related documents are complied with whilst handling NATO-owned information. And last but not least, NAC plays the role of an entity responsible for monitoring compliance with, and execution of, Policy accompanied by supporting Directives by NATO civil and military bodies; coordinated implementation of the Policy objectives; and appropriate coordination among all NAC Policy bodies (MC, Political Committee, NATO Security Committee, NATO C3 Board and NATO Archives Committee) dealing with individual elements of IM (NIMP, 2007, p. 1–3). The roles and responsibilities of various Alliance political and military levels are described in detail in IKM Directive and INFO OPS Doctrine.

The Russian perception of the world presented by political and military leadership includes its inherently hostile and unstable nature (Hedenskog, Person and Vendil Pallin, 2016, pp. 114–119). The Russian National Security Strategy and Russian Military Doctrine list a number of threats posed by entities from all directions. International and domestic instability may be countered by the implementation of "a dual complementary strategy: to assert Russian sovereignty internationally while safeguarding regime security at home through ever tighter control" (Westerlund, 2018, p. 35). However, considering threats and challenges existing in the Information Environment, the problem of countering such phenomena was described very poorly in the above mentioned documents. One may conclude that that "until now, recognising the reality of the information threat, the Russian military-political decision-makers are trying to independently master the new kind of technological confrontation utilizing the armed forces and military technologies" (Pietkiewicz, 2018, p. 515).

Decision-making in Russia is highly centralized, and President Vladimir Putin dominates Russia's decision-making, to include military and security issues. The Russian president is the Supreme Commander in Chief of Russian military. The Russian Ministry of Defence, subordinate to President Putin, is responsible for the implementation of the presidential policy within the military. The defence minister owns the legal authority to supervise and guide operations of the General Staff. The General Staff's primary mission is to ensure the military security of the Russian Federation, which means to protect the vital interests of the state and society from threats posed by internal and external actors. The General Staff is in charge of monitoring and analysing the threat environment and developing strategic and operational plans considering equipment, mobilisation, employment, command and control of the armed forces. The 2013 presidential edict describes General Staff missions, functions, and its scope of responsibilities that was broadened to encompass coordination of all activity undertaken by federal executive organisations to ensure defence capability and security (DIA, 2017, p. 24).

Compared to the Western (NATO) ideas of command and control scope of responsibilities, the Russian chief of the General Staff has been given much more authority than any flag grade officer representing the Western military. He is in charge of long-term planning duties that may be perceived as equivalent to the U.S. Office of the Secretary of Defence. General Valery Gerasimov, currently occupying the post, has oversight of strategic transportation which seems to be equivalent to the U.S. Transportation Command. He also supervises force doctrinal and capabilities development, as well as equipment procurement for all branches of the Ministry of Defence. The chief of the Russian General Staff does not exercise operational control of the force, but he does have peacetime control of the Glavnoye Razvedyvatelnoye Upravleniye (Main Intelligence Directorate, commonly known as GRU), being a directorate of the General Staff (Bartles, 2016, p. 30).

Russia perceives information warfare as “a key means of achieving its ambitions of becoming a dominant player on the world stage” (Chekinov and Bogdanov, 2013). Therefore, since 2010, the Russian military priorities comprise the development of forces and means for a holistic concept for ensuring information superiority, during peacetime and wartime, which is known as *information confrontation* (Prudnikov, 2008). A good example of the developments implemented in the Russian military so far was the announcement of the chief of General Staff considering the exercise KAUKAZ-2016. He stated that ‘information operations troops’ took part, for the first time, in this strategic command staff exercise. Their participation demonstrated “Russian military commitment to controlling the information domain” (DIA, 2017, p. 38).

One of the latest instruments applied by Russia in the information domain are the cyber-enabled psychological operations. They support the achievement of Russian strategic and tactical information warfare objectives. These techniques refer to “compromising networks for intelligence information that could be used to embarrass, discredit, or falsify information. Compromised material can then be leaked to the media at inopportune times" (DIA, 2017, p. 39). This kind of operations includes the application of hacktivists, trolls and bots.

Russian intelligence services have been known and recognized for co-opting or masquerading as other hacktivist groups. Difficulty of attribution and the level of anonymity provided make these groups easily appeal to Russia. Moreover, the government employs an army of paid trolls, online commentators manipulating or trying to change the perception of a given story in Russia's favour. Russian Troll Army, called the Internet Research Agency (Russian IRA), is an organisation funded by state. Its blogs and tweets support the narrative of the Kremlin. There are also other ways of manipulation used by Russia in the information space: one of them is affecting the domain through the bots. They are "automated pushers of content on social media. These bots vary in sophistication and can continuously push content or imitate real life patterns. Bots can drown out unwanted content or push a specific message. Bots have the ability to overwhelm the information space and discourage readers from looking for real content" (DIA, 2017, p. 40).

5. Conclusions

Although certain terms seem to have a commonly understood meaning, there are concepts and ideas that may be interpreted in many different ways, even within one organisation or entity. *Information* happens to be such a concept as far as the NATO interpretations are concerned. The research has led to the following findings:

(1) *Information* as an element of military operations, e.g. Information Operations, is an instrument of influencing a selected Target Audience. Certain related definitions, *vide* Information Superiority, may suggest a more active, or even aggressive, approach towards the operational (information) environment and its actors. If it is defined in the frames of Information and Knowledge Management, it takes on a completely different form, connected to management, not operations.

(2) The two concepts – INFO OPS and IKM are not contradictory; they are two alternative perspectives of information perception complementing the whole spectrum of the term interpretations.

(3) Diversity of objectives, applied principles, played roles and assigned responsibilities has been clearly indicated – both internally, and externally.

(4) The role of information seems to be completely different as far as the Russian perception of the *information warfare* / *information confrontation* is concerned. In the Russian construct all the information-related activities are not limited to wartime or peacetime, they tend to reflect the ongoing campaign taking place regardless of the nature of relations with adversary or potential adversary.

(5) Russia does not consider information warfare as a tactical, short-term operation characteristic for wartime, this is a constant feature of modern political and social reality, especially in terms of exercising any form of leadership, to include the military one.

Summing up, the research shows that the perceptions of information presented by the Alliance and the Russian Federation differ substantially. The roles played by information in exercising military leadership vary as well. Considering Russian perception of information, its main concept is included in the fundamentals of information confrontation as a form of warfare. The Allied interpretation of the term focuses on data, intelligence and knowledge represented in many diverse forms.

The study contributes to the research field as the differences in the information perception have not been compared in such a set yet, especially internally within the Alliance – Information/Knowledge Management and Information Operations. Moreover, the wider context of Russian understanding of the apparatus applied within the Information Environment, though identified, has not been collated with the Allied approach either.

The way ahead, as far as further research in this area is concerned: firstly, it may include the evolution of the perception of information reflected in various allied documents as well as the further implementation (or alteration) of the Russian information confrontation concept; secondly, the practical application of theoretical fundamentals, to include the assessment of the methods' efficiency on the basis of selected case studies.

References

AAP-6 (2018). *NATO Glossary of Terms and Definitions*. NATO Standardization Office.

AJP-3.10 (2015). *Allied Joint Doctrine for Information Operations*, Edition A, Version 1. NATO Standardization Office.

Averin, A. (2018), Russia and its many truths. In Althuis, J., & Haiden, L. (Eds.), *Fake News: A Roadmap* (pp. 59–67), Riga: NATO StratCom Centre of Excellence & The King's Centre for StratCom.

Bartles, Ch. K. (2016). Getting Gerasimov right. *Military Review: The Professional Journal of the U.S. Army*, January-February, 30–38.

Chekinov, S. G., & Bogdanov, S. A. (2011). The influence of the indirect approach on the nature of modern warfare. *Voyennaya Mysl*, 6.

Chekinov, S. G., & Bogdanov, S. A. (2013). The nature and content of a new generation war. *Voyennaya Mysl*, 4.

DIA (2017). *Russia – Military Power: Building a Military to Support Great Power Aspirations*. U.S. Defense Intelligence Agency.

Fallis, D. (2015). What is disinformation. *Library Trends*, 63(3), 401–426.

Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?. *Small Wars and Insurgencies*, 27(2), 282–301.

Giles, K. (2016). *Handbook of Russian Information Warfare*. Rome: NATO Defence College.

Hedenskog, J., Persson, G., & Vendil Pallin C. (2016). *Russian security policy*. In Persson, G. (Ed.), *Russian Military Capability in a Ten-Year Perspective – 2016* (pp. 97–132). Stockholm: Swedish Defence Research Agency.

Jowett, S. G., & O'Donnell, V. (2015). *Propaganda & Persuasion*. London.

Kartapolov, A. V. (2015). Lessons of military conflicts and prospects for the development of means and methods of conducting them: Direct and indirect actions in contemporary international conflicts. *Vestnik Akademii Voyennykh Nauk*, 2.

Kuleshov, Y. (2014). Information-psychological warfare in modern conditions: Theory and practice. *Vestnik Akademii Voyennykh Nauk*, 1(46).

Kvachkov, V. (2004). Russia's special purpose forces. *Voyennaya Literatura*.

Lis, A. (2014). Knowledge creation and conversion in military organizations: How the SECI model is applied within armed forces. *Journal of Entrepreneurship, Management and Innovation*, 10(1), 57–78.

Lis, A. (2015). Instytucjonalizacja zarządzania wiedzą w organizacjach wojskowych na przykładzie NATO. In Mikuła, B. (Ed.), *Współczesne tendencje w zachowaniach organizacyjnych* (pp. 209–214). Kraków: Uniwersytet Ekonomiczny w Krakowie.

Madeira, V. (2014). Haven't We Been Here Before?. Institute of Statecraft.

MC 0422/5 (2015). *NATO Military Policy for Information Operations*. North Atlantic Military Committee.

McManus, Ch., & Michaud, C. (2018). Never mind the buzzwords: Defining fake news and post-truth. In Althuis, J., & Haiden, L. (Eds.), *Fake News: A Roadmap* (pp. 14–20). Riga: NATO StratCom Centre of Excellence & The King's Centre for StratCom.

Modrzejewski, Z. (2015). *Operacje informacyjne*. Warszawa: Akademia Obrony Narodowej.

NIMP (2007). *NATO Information Management Policy*. North Atlantic Council.

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

PDIM (2008). *Primary Directive on Information Management*. North Atlantic Council.

Prudnikov, D. P. (2008). State information policy in the defense area: An initial definition. *Military Thought*, 17(2).

Pynnoniemi, K., & Racz, A. (2016). *Fog of Falsehood: Russian Strategy of Deception and the Conflict in Ukraine*. FIIA Report No. 45.

Slipchenko, V. (2013). Information resources and information confrontation. *Armeyskiy Sbornik*, October.

Snegovaya, M. (2015). *Putin's information warfare in Ukraine: Soviet origins of Russia's hybrid warfare*. Institute for the Study of War.

Suiter, J. (2016). Post-truth politics. *Political Insider*, 7(3), 25–27.

Tsvetkova, M., & Devitt, P. (2016). Russian editors 'fired over stories that irked officials'. Reuters.

Westerlund, F. (2018). Force or modernization. In Deni, J. R. (Ed.). *Current Russia Military Affairs*: *Assessing and Countering Russian Strategy, Operational Planning, and Modernization* (pp. 35–39). U.S. Army War College.