Volume 2 Issue 1 2015

JOURNAL OF CORPORATE RESPONSIBILITY AND LEADERSHIP

MILITARY LEADERSHIP

Military Leadership in the Context of Challenges and Threats Existing in Information Environment

DOI: http://dx.doi.org/10.12775/JCRL.2015.001

TOMASZ KACAŁA

Allied Joint Force Command Brunssum, The Netherlands

e-mail: tomasz1975@yahoo.com

Abstract: The aim of the paper is to present the role of a military leader in engaging the challenges and threats existing in the Information Environment (IE). Military leadership is crucial for the functioning of a particular form of hierarchical institution, namely the armed forces, in their external surrounding called Operational Environment (OE). A specific type of OE is Information Environment (IE) characterized by the three dimensions: physical, informational and cognitive. Moreover, its characteristics include the occurrence of a number of challenges and threats. The most important challenges include: overabundance of information, unstructured information, problematic value of information and low information-related competences of its users. In turn, the most important of the threats identified in the IE are disinformation and propaganda. The role of an effective leader is to prevent, and if it is impossible, to alleviate the consequences of the challenges and threats that may disrupt or even prevent the achievement of the objectives set by an organisation.

Keywords: military leadership; operational environment; information environment; disinformation; propaganda; social communication.

1. Introduction

Military leadership is a fundamental element enabling the effective and efficient functioning of armed forces in Operational Environment (OE). The environment, as the external surrounding of a hierarchical institution, is a system of highly dynamic character. OE is hereby understood, according to the latest trends observed in modern Art of War, as a set of conditions, circumstances and factors affecting the use of the relevant capabilities and decisions taken by a leader/commander. It has many dimensions: physical (land, sea, air and space), informational (relating to Information Environment, including cyberspace), and systemic (relating to military, political and economic systems and subsystems). It is also the space where actual and potential opponents, as well as other actors that are not directly involved in supporting any of the conflict parties, function, take their actions and realise their goals. Hence, the proper understanding of Operational (Information) Environment and of the events that take place in there, and then the appropriate shaping of O(I)E is a prerequisite for success of such measures (operations). Responsibility in this regard is inextricably linked with the competencies of a leader. It is expressed through the role played by him/her in the decision-making process. It is of the key importance, in this context, to provide leaders with appropriate knowledge, especially within their preparation for making proper decisions. The knowledge gained and made available to leaders as a result of the process includes factors and phenomena of various nature which affect or may affect ongoing or planned activities. Some of these elements are completely independent of will or intention of any potential conflict party. Interference with the process of social communication, emerging from natural causes, may be the best example of such a situation.

However, certain phenomena are the result of planned actions aimed at influencing the level of situational awareness of an opposing party. Such actions should certainly include undertakings occurring in the field of propaganda and disinformation. Their aim is, in fact, to shape the recipient's knowledge in a misleading way enabling serious implications with respect to the accuracy of decisions. In extreme cases, the results of the wrong decisions taken on the basis of incorrect assumptions may lead to total failure. Therefore, countering disinformation and propaganda is one of the key conditions for the success of the activities carried out in OE, especially in its informational dimension

(IE). Countering actions taken in the field of propaganda and disinformation should be comprehensive in nature. The complexity of the activities should be expressed inter alia in taking both ad hoc (hasty) activities (in response to specific manifestations of adversary information activities) and long term (building knowledge on the mechanisms of disinformation and propaganda). It is a prerequisite for effectiveness characterising this type of actions resulting from the need for a holistic approach to all the events occurring in Information Environment.

The aim of the paper is to present the role of a military leader in engaging the challenges and threats existing in the Information Environment (IE). The author will make an attempt to describe the most relevant factors affecting IE and thus shaping the process of social communication within and outside a hierarchical organisation. The most important elements that require further analysis in terms of a military leader's involvement are disinformation and propaganda as intentional, planned and directed activities aimed at the achievement of very specific objectives. Successfully exercised military leadership, using selected instruments (e.g. counter-propaganda techniques), seems to be the key to mitigating the potentially hostile effects caused both by disinformation and propaganda and by other phenomena of IE.

2. Information Environment

Information Environment itself is characterised by a high level of complexity and far-reaching multidimensionality. It is often understood as the space where information is produced, acquired, processed and transferred from senders to designated recipients. Information Environment has three dimensions:

- physical – e.g. ICT infrastructure;
- informational – information content and its effects;
- cognitive – the way information is received (JP 3–13, 2012, p. x).

The physical dimension is composed of command and control systems, key decision makers, and supporting infrastructure that enable individuals and organisations to create effects (JP 3–13, 2012). Physical dimension involves physical platforms and communications networks that connect them as well as a number of elements which include people (individuals and groups), infrastructure, publications and periodicals,

computers, laptops, smartphones, tablets and other such items. Physical dimension, in practice, is a network available regardless of national borders and economic or geographical barriers.

The informational dimension specifies where and how information is collected, processed, stored, disseminated, and protected (JP 3–13, 2012). Informational dimension concerns not only the place of collection, processing, storage, transmission and protection of information but also the methodology applied. The dimension is a platform for directing a defence system and commanding the military, which results in actions affecting the content of information and its flow.

The cognitive dimension encompasses the minds of those who transmit, receive, and respond to or act on information (JP 3–13, 2012). Cognitive dimension also includes actions of those individuals. This applies to the processing of information, its perception, assessment and making decisions by individuals or groups. It should be taken into account that there are many factors involved – e.g. individual beliefs and cultural background, social norms, threats and fears, motivations, emotions, experience, morality, education, identity and ideology. Defining these factors, affecting OE(IE), is key to understanding how best to influence decision-makers and achieve desired results. This dimension is the most important part of IE.

3. Challenges and threats existing in Information Environment

Modern Information Environment is extremely complex, heterogeneous and disordered. It is characterised by the occurrence of a number of challenges and threats. Phenomena understood as communication challenges are the challenges naturally occurring in the course of social communication process. The most visible of these are: overabundance of information, unstructured information, problematic value of information and low information-related competences of its users (Głowacka, 2013, pp. 2–3). On the other hand, one can define the threats as intentional human activities aimed at influencing the level of another human being's consciousness or awareness of whole social groups in order to provide the influencing agent with specific benefits. It is often connected with the negative consequences incurred by an object of such an impact. The most significant threats that may occur in Information Environment are: disinformation and propaganda (Kacała, 2015, pp. 49–66).

One of the key challenges is overabundance of information. It means information overload or explosion, information bomb, and the flood of information. The phenomenon occurrence has increased since the mid-twentieth century. But nowadays, in connection with the development of web resources, especially social services and resources, it is gaining significant momentum. As a result, in opinions of information users, "information noise" is created. It means imbalance between the amount of information provided and the possibility of its processing by a human being. The so-called informational stress (cognitive stress or info-stress) appears then. Another phenomenon present in the modern IE is unstructured or disordered information – information that is chaotic, incoherent or distracted. It means atomization and fragmentation of information – information occurs without context in the forms of isolated pieces. Problematic value of information is also a major challenge present in IE. We are dealing here with very different causes of low quality and value of information. This is primarily a problem of unreliable and outdated sources of information connected with lack of informational documentation and presence of "toxic" information bearing poisonous and harmful content (e.g. pornography, racism, violence, intolerance, "quasi-science" and so on). The last of these phenomena is low information-related competences of its users (i.e. information illiteracy). In the information society, it is important to have an ability to search, select and use information resources and information itself for development of own knowledge. Unfortunately, many information users are not able to properly use the available resources.

In the case of disinformation and propaganda we deal with a preplanned actions conducted for certain purposes. General concept of disinformation refers to certain types of information being, in fact, its opposite. It is false, deceptive and misleads the recipient. The main interpretation assumption represented by the notion of "disinformation" is its purposefulness – false information is provided in order to achieve certain effects, give the recipient an apparent knowledge, useless or even harmful, which then makes him or her take wrong decisions beneficial for the source (Wrzosek, 2005, p. 8). Whereas propaganda, according to some authors, may be defined as clever use of images, slogans and symbols referring to our prejudices and emotions; it consists in communicating certain point of view in order to induce the recipient to voluntarily adopt this point of view as his own (Pratkanis and Aronson, 2004, p. 17). Others describe it as a technique of influencing the

behaviour of citizens, controlling and manipulating public opinion. It is based on the latest scientific achievements and results of empirical research in social psychology, sociology, political science, theory of communication and other social sciences (Dobek-Ostrowska et al., 1999, p. 32). In conclusion, propaganda may be considered as a set of social communication activities aimed at influencing the target audience's state of consciousness in order to provide the sender (source) with specific benefits (advantages).

An interesting point of view on challenges and threats existing in IE has been included in newly developed Polish *Doctrine for Information Security of the Republic of Poland* (draft as of 24 July 2015). The draft document that has been prepared by the National Security Bureau this year not only distinguishes threats and challenges but also chances and risks related to information security. Their typology is based on two dimensions: external and internal. Although the doctrine itself is more focused on the state and its surrounding than on the role of (military) leadership, it still can be considered as a valuable source of knowledge about the characteristics of Information (Security) Environment (Doktryna, 2015, pp. 6–8).

4. Military leadership and its role in shaping Information Environment

The proper understanding of the role played by military leadership in the context of challenges and threats appearing in Information Environment requires clarification of the "leadership" notion. It is closely related to the position and role performed by the individuals heading human teams who are called leaders (Łydka, 2014, p. 23). According to theoreticians dealing with the above mentioned issues, leadership is conditioned by four basic elements: human resources, values, unequal distribution of power and the ability to use it (Boguski, 2003, pp. 29–30). With regard to human resources, the essence of leadership is expressed in the involvement of people being the primary form of organisational activity. Effectiveness of actions undertaken by an organisation depends on acceptance and support provided to leadership by its members. In turn, values are closely linked to the so-called organisational culture. Leadership is associated with certain values defining canons of human attitudes and behaviours of an organisation's members. While unequal

distribution of power is connected with a particular role designated for a leader and his/her relation with members of an organisation – both those who support the leader, as well as those who may present different opinions. It should be noted that this element can be a potential source of conflict emerging within organisation. Last but not least important element is the ability to use power properly. Effective leaders use it in a selective manner, depending on situation. They strive for flexibility of response, especially in terms of possible conflicts.

There are many definitions of leadership that reflect various viewpoints (references) – e.g. sociology or theory of management. The common denominator, however, is the understanding of leadership as a set of specific skills that should be attributes of leaders in all organisations. The analysis of the subject matter literature may lead to the conclusion that so far, very often, the concept of "leadership" and "command" have been treated synonymously, which does not seem to be the right approach. The definition developed by Kanarski, Pęksa and Żak describes leadership as a certain ability, skill or trait of winning followers, influencing people, and creating a vision of development and encouraging people to take actions (to be active). However, its most important element, defining the essence of actual and natural leadership, is a voluntary organisation, gathering people around a leader and motivating them to achieve specific objectives (Kanarski et al., 1998, p. 47). Leadership is, therefore, based on the principle of voluntary commitment. It is, in fact, the negation of the command concept applied within the military structures as a specific type of direction/management closely related to rigour of tasks feasibility.

In this context, a leader plays a very important role in shaping Information Environment. The best example of the role importance is his or her participation in social communication (e.g. in Strategic Communication). The communication may take place within a hierarchical organisation and also serve to disseminate intended messages outside its structures. In the case of communication conducted within an organisation, a leader acts as a reliable source of information that enables building a community composed of members consciously fulfilling tasks for the purpose of organisation. In this case, the goals of individual members of organisation are consistent with the objectives of globally understood system established by that organisation. Leader acts as an entity initiating desired actions of individual components of the system and a motivational factor which also directs efforts of

individual community members within the framework of the objectives set for the purpose of the whole system. In the case of external environment of the system (organisation), the task of leader consists in striving for creation of conditions enabling achievement of the aforementioned objectives despite the existence of challenges (phenomena emerging due to natural causes that are characteristic of social communication process) and threats (situations and actions initiated by certain entities with the intention of interference with or disruption of organisational objectives' achievement and, at the same time, supporting achievement of the goals set out by these entities). The role of leader is not confined solely to the act of communicating with certain audiences but also includes implementation of undertakings eliminating negative effects of existing or emerging threats (e.g. attempts to mislead or misinform members of an organisation or draw their attention to objectives other than those established by a given organisation).

5. Responding to challenges and countering threats

Military leadership plays an important role in responding to both the challenges and the threats existing in Information Environment. In relation to the phenomena occurring in the environment in a natural way, as a side effect of social communication, a leader essentially plays the role of a moderator – an entity levelling the negative effects of identified challenges. In response to overabundance of information, a leader should be a "safety valve" (controller) to protect the members of an organisation (e.g. armed forces) from data overload. The task of leader is to prevent the occurrence of "information noise" disturbing the proper conduct of planning and decision-making process. It is possible by the means of implementation, appropriate use and the monitoring of measures taken to regulate the flow of information. The measures may be both of a technical nature (e.g. information management and control of information circulation) and the procedural ones (e.g. establishment of information handling procedure in the framework of an organisation as its set mode of operation). With regard to dealing with unstructured information, the role of a leader is based on implementation and proper management of the structures (cells) verifying analytical value of information disseminated within an organisation. In the case of information fragmentation, properly directed structures should initiate the process

of information replenishment and ordering. The ultimate authority to verify the achieved degree of informational order and, by this means, to authorize information for dissemination should be given to managing entity (leader). Similar situation occurs in the case of problematic value of information. In case of doubt on reliability and validity and possible "contamination" of information, a leader should initiate a re-check procedure (verification) concerning received information, particularly in relation to the sources of the information. Organisational elements responsible for assessment and evaluation of the external environment (e.g. military intelligence) are crucial in such a situation. Appropriate coordination of their efforts with internal analysis cells lies within responsibilities of an effective leader. Unfortunately, there is an area where a leader may have the most limited freedom of direct impact. The area includes low information-related competences of its users. Actions taken in relation to this challenge should be long-term in nature and consist in the constant raising of recipients' awareness through an education process assisted by ad hoc (short-term) training events and courses.

Countering threats occurring in Information Environment, a leader should take both short-term measures into account and implement undertakings that are long-term in nature. With regard to propaganda and disinformation, some techniques have been developed. They are successfully applied in the context of military Psychological Operations (PSYOPS) and, therefore, it appears advisable to use them in order to counter the above mentioned threats. The techniques include: direct refutation, indirect refutation, diversion, silence, forestalling and minimization. Whereas in terms of long-term activities, there are some fundamental forms of counteracting threats that include shaping IE by the use of restrictive measures and education based on reasonable assumptions developed in the course of research process (FM 33–1–1, 1994, pp. 12.12–12.13).

Direct refutation involves detailed verification of propaganda or disinformation content to demonstrate its falsity. This technique is used when, on the basis of analysis, one finds out that the disseminated message is untrue. Direct refutation should be characterised by credibility and be implemented as soon as possible in order to minimize the effects of propaganda or disinformation. The only drawback of this technique is related to the fact that it may result in drawing attention of potential recipients to propaganda/disinformation messages.

Indirect refutation includes introduction of a new set of themes (new content) which undermine the credibility of disinformation or propaganda. The basic form of its implementation consists in suggesting target audience the way to interpret false information disseminated by potential adversary and its aim is undermining his or her credibility. Moreover, application of the technique does not strengthen (replicate) the contents of propaganda or disinformation.

Diversion essentially means dissemination of messages on issues other than those raised by propaganda or disinformation. Message contents should arouse greater interest of the recipients and thereby divert their attention from the contents of propaganda or disinformation.

The "silence" technique is based on the assumption that a given disinformation/propaganda message does not require any action or counter-message. This technique is used, among others, in case of a single act of disinformation or propaganda. The solution may be applied as a result of limited knowledge of the countering entity and its intention to avoid adverse or even harmful effects of potential response. The use of this technique should be preceded by thorough analysis of all the relevant factors and possible results.

Forestalling consists in an earlier response of countering entity to a crisis situation. It includes reaching specific audiences with the right message before an adversary agent does. This technique requires careful analysis of a potential adversary and knowledge of its capabilities, particularly in relation to dissemination of its narrative. It combines some elements of hasty measures and long-term undertakings (e.g. constant analysis of disinformation and propaganda).

Last but not least technique to counter threats present in IE is minimization. It is also one of the most demanding techniques because it involves confirmation of at least part of the information provided by a potential adversary and, at the same time, shifting the accent of its meaning. The technique is used when one cannot deny the presented message, discredit its credibility or remain silent with respect to given situation. Minimization may take three forms: emphasizing fragments of message that are beneficial to the recipient; suggesting that complete information will be provided later (after finding all the facts); confirming certain contents and raising other topics/issues.

However, the threats characterizing Information Environment should be countered mainly by means of long-term activities. One of the two kinds of such activities is the use of preventive measures

– limiting the dissemination of disinformation or propaganda messages. This is primarily related to constant dissemination of true and accurate information among members of a group (organisation). The disseminated messages should refer to current situation, the functioning of organisation, its goals and actions taken by its management (leaders). The key role, in this regard, is played by leaders using available internal communication channels with the intention to prevent formation of so-called "information vacuum" that can easily be filled with rumours or false, incomplete or unproven information. The proper organisation of internal communication within the organisation is one of the most important responsibilities of an effective leader.

Another activity conducted in the frames of countering IE threats is proper education of given community (staff, members of a group) in terms of knowledge about methods and mechanisms of propaganda and disinformation. Understanding a broader context of organisational functioning, common goals and tasks is crucial for proper perception of planned actions undertaken by potential adversaries in Information Environment. Disinformation and propaganda always have their goals and, like each information activity, are disseminated via certain channels, have their target audiences, respectively constructed content, as well as the intended effect. Determination of these components allows for effective protection against the harmful effects of such activities.

6. Conclusions

Exercising military leadership as a form of relations between elements of a system (armed forces) is heavily dependent on the factors affecting its external environment (Operational Environment). In one of its dimensions, the informational one, the environment reaches a very high level of complexity, which is the basis for taking into account another autonomous subsystem of factors and relations referred to as Information Environment. Information Environment also has its dimensions relating to various aspects of information and related processes (i.e. cognitive process).

Information Environment is characterized by a number of phenomena that may affect the functioning of a hierarchical organisation (e.g. armed forces). These phenomena may be of natural character and may appear during the communication process as its by-products

(unintended effects). They may also be intentional and thus resulting in situations aimed at achieving intended informational effects. The phenomena occurring spontaneously are called challenges, while in the case of deliberate and pre-planned activities initiated by other entities operating in Information Environment one should consider them as threats.

The proper functioning of the aforementioned organisations in Information Environment depends on adequate leadership. By this we mean specific actions taken by a leader in the context of mitigating the negative effects of the challenges and threats emerging in the surrounding of their organisation (system led by them). Actions taken by a leader to face the challenges essentially consists in controlling the quality of information entering the system and controlling relevant processes (e.g. protection against overload of information, improving quality of information or elimination of fragmented information received from "toxic" sources). Undertakings implemented in response to the IE threats include the entire spectrum of activities which are both hasty and long term in nature. Hasty measures, also referred to as techniques to counter propaganda and disinformation, include: direct refutation, indirect refutation, diversion, silence, forestalling and minimization. Long-term activities encompass education of group (organisation) members on possible ways to influence them through the activities of propaganda and disinformation. The key is explanation of objectives, principles, methods and techniques used in propaganda and disinformation, and reduction of their impact on the functioning of the whole organisation.

The subject of these considerations was military leadership in the context of challenges and threats existing (emerging) in Information Environment. The essence of such leadership is playing the role of a leader-organiser and a leader-participant. The leader-organiser properly organises the functioning of an organisation (community of members), especially in terms of its internal and external communications. The leader-participant takes an active part in the process of social communication (e.g. in Strategic Communication) being an author and a sender of specific messages and thus shaping a suitable environment to achieve success and organisational objectives, both in its internal and external environment.

The role of effective (military) leadership should consist in development of a universal, cross-functional and multi-level concept of

challenging all the phenomena existing and occurring in the Information Environment. The military leader is the initiator and conductor of all the activities taken in this regard. He or she should be the real "information and influence leader". It, of course, requires a high level of knowledge, competence and personal involvement. The military leader (commander) does not to know all the details and techniques necessary to shape different dimensions of his or her operational space but, first of all, needs to have a clear vision of the end state he or she wants to achieve. Otherwise no objective will be achieved and no dimension of Information Environment will be shaped in favour of the operational success.

References

Boguski, J. (2003), *Przywództwo i władza*, OTW im. Adama Chętnika, Ostrołęka.

Dobek-Ostrowska, B., Fras J., Ociepka B. (1999), *Teoria i praktyka propagandy*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław.

Doktryna bezpieczeństwa informacyjnego RP (2015), BBN, Warszawa. Retrieved from https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf (accessed 12 November 2015).

FM 33–1–1 (1994), *Psychological Operations Techniques and Procedures*, U.S. Department of Defence, Washington.

Głowacka, E. (2013), "Ekologia informacji – sposób na choroby informacyjne?" Retrieved from http://konferencja.biblio.cm.umk.pl/fileadmin/pelne_teksty/nowy_ekologia_inf.doc (accessed 21 July 2015).

JP 3–13 (2012), *Information Operations.* 27 November 2012 Incorporating Change 1 20 November 2014, US DoD, Washington D.C. Retrieved from http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf (accessed 12 November 2015).

Kacała, T. (2015), "Dezinformacja i propaganda w kontekście zagrożeń dla bezpieczeństwa państwa", *Przegląd Prawa Konstytucyjnego*, No. 2(24).

Kanarski, L., Pęksa, R., Żak, A. (1998), *Przywództwo wojskowe: Tradycje, teoria, praktyka*, Wydawnictwo Klio, Warszawa.

Łydka, W. (2014), *Przywództwo wojskowe*, Wojskowe Centrum Edukacji Obywatelskiej, Warszawa.

Pratkanis, A., Aronson, E. (2004), *Wiek propagandy*, Wydawnictwo Naukowe PWN, Warszawa.

Wrzosek M. (2005), *Dezinformacja jako komponent operacji informacyjnych*, Wydawnictwo Akademii Obrony Narodowej, Warszawa.