Research Journal 28, No. 4 (2021), pp 59-69

October-December

Justyna LIPIŃSKA¹

STRATEGIC COMMUNICATION IN THE FACE OF CONTEMPORARY THREATS TO THE INFORMATION ENVIRONMENT

Citizens' involvement in social life is essential to the functioning of civil society. This takes place when citizens are duly informed and involved in the activities of public institutions. To realize this, it is necessary to develop an extensive information policy that integrates a given ministry's strategic communication expectations. The aim of this article was to describe strategic communication in relation to the implementation of a systemic method of communication in the army together with its structures in the larger society, including allied countries. This description was carried out against the background of contemporary threats to the information environment. The following research problem was posed: How are the assumptions of strategic communication implemented against the background of contemporary threats to the information environment? Qualitative analysis was the research method used, and the technique used was the analysis of source documents.

Keywords: international security, strategic communication (StratCom), threats to the information environment.

1. INTRODUCTION

The process of managing the image of the armed forces is, on the one hand, strongly regulated by regulations and instructions, and on the other – free and devoid of detailed solutions due to changing political, military, economic, social and information conditions. The need to systematically inform the public about the activities of the armed forces was especially noticed during the conflict in Yugoslavia in 1992². In turn, in the Polish armed forces it only happened in 2004. The image of the army in society, like many other public institutions, translates into for its smooth operation. A modern and professional army needs

_

Justyna Lipińska, DSc PhD, Associate Prof., The Faculty of Management and Command, The War Studies University, l. gen. A. Chruściela "Montera" 103, 00-910 Warszawa-Rembertów; e-mail: j.lipinska@akademia.mil.pl. ORCID: 0000-0001-8233-6971.

² The war in Yugoslavia was very well prepared in terms of propaganda. The aim of this campaign was to shape the belief that before the start of the NATO attack in Kosovo, there had been a humanitarian catastrophe - mass murder and expulsion of Albanians from the provinces, that the victims are Albanians and the perpetrators are Serbs. Military intervention to put an end to this catastrophe was to become the responsibility of aspiring states to recognize them as major human rights defenders. The media became involved in promoting this position, especially in the countries participating in this project.

high-class specialists. By sending such a message to the public, he has the opportunity to expand his area of searching for suitable candidates for the service. Another important element related to the activities of the military is cooperation between the military unit and entities in the environment. Mutual understanding is a guarantee of tolerance for both sides, and the basis of this tolerance is knowledge that today is obtained primarily from the mass media. Living in the information society, the social environment not only uses the benefits of technology for consumption or entertainment, but also perceives it as a source of information and knowledge about the surrounding world. Armed forces, using the potential of the mass media, must provide the public with answers to several basic questions: what are their tasks now? What direction are they going? What are the benefits of their functioning for society? These questions are answered through strategic communication. As noted by Ansgar Zerfass, Dejan Verčič, Howard Nothhaft and Kelly Page Werder.

Communication can play a distinctive role for the formulation, revision, presentation, execution, implementation, and operationalization of strategies. While there are many ways to investigate these research objects, strategic communication as a discipline takes the perspective of the focal organization/entity and its calculus to achieve specific goals by means of communication under conditions of limited resources and uncertainty(Zerfass, Verčič, Nothhaft, Werder, 2018).

In turn, Hallahan, Holtzhausen, van Ruler, Verčič and Sriramesh define strategic communication "as the deliberate use of communication by an organization in order to fulfill its mission" (Hallahan, Kirk, Holtzhausen, Derina, Ruler, Betteke, Verčič, Dejan, Sriramesh, Krishnamurthy, 2007). Necessary for the survival and lasting success of an entity. Strategic communication is a deliberate use of communication by an organization or other entity to conduct discussions of strategic importance to its goals (Zerfass, Verčič, Nothhaft, Werder, 2018).

In the military, as part of strategic communication activities, psychological operations (PSYOP), information operations (IO) and psychological warfare are used. They are examples of the deliberate use of communication by a government or military organization to fulfill its mission, and therefore have different understandings of the concept of strategic communication (Wallenius, Nilsson, 2019).

The research objective presented in this article was to characterize NATO's strategic communication, which consists in the implementation of a systemic method of communication between the army and its structures with the social environment in the allied countries against the background of contemporary threats to the information environment.

Therefore, an answer was sought to the following research problem: how are the assumptions of strategic communication implemented in NATO against the background of contemporary threats to the information environment?

They want to get an answer to a given research problem, a qualitative analysis was used with the use of the technique of source documents analysis. Therefore, for the purposes of the analysis, the characteristics of the strategic communication areas were made and the allied normative documents were reviewed, taking into account the contemporary requirements of the information environment.

2. CONTEMPORARY REQUIREMENTS OF THE INFORMATION ENVIRONMENT

When analyzing the information environment in the context of operations conducted in it by the armed forces, first of all, it is necessary to identify the threats present in it. This approach allows for the definition of needs in relation to the prevention, counteraction and neutralization mechanisms. At the same time, it means the necessity to define tasks for individual military capabilities and communication functions in times of peace, crisis and war, as part of everyday functioning and as part of operations (Decision No. 478 / MON of 8 December 2014)³.

The armed forces are an element of every state, therefore all actions aimed at undermining the decisions taken as part of managing defense ministries, disrupting the decision-making process, weakening the image and competences of top-level commanders, or negating processes aimed at modernizing military equipment, have an indirect impact on the functioning and security countries. Therefore, it is important to understand the functioning of the information environment and the factors surrounding it, influencing the proper risk analysis.

An important group, important from the perspective of this analysis, is the area of direct information threats. The most important of them include:

- 1. image threats,
- 2. cyber threats,
- 3. military threats (NATO Military Policy On Strategic Communications, SH/SAG STC/AM/17-318278, 2017).

3. IMAGE THREATS

Image threats may result in a reduction or complete loss of credibility of the activities undertaken by the ministry (Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, 2014). Even a small loss of credibility may cause difficulties in the implementation of the ministry's narrative prepared in accordance with the strategic communication (StratCom) guidelines, which may significantly reduce the effectiveness of the communication process. Image threats may result from own activities, neutral environments, as well as hostile to the activities undertaken by the ministry. Accidental risks, i.e. errors resulting from insufficient coordination or inappropriate use of communication skills, are by far the easiest to eliminate. The solution seems to be the implementation of the strategic communication guidelines approved for implementation and the proper coordination of the activities of communication capabilities and tools as well as military actions having an indirect impact on the cognitive and information sphere of the information environment. A much more dangerous scenario seems to be an event when the intended operational activities will have a negative communication effect (e.g. accidental civilian casualties as a result of an operation). Therefore, building the awareness of commanders of even the lowest rank (platoon, company, battalion) in terms of strategic

³ Communication skills and functions are defined in point 3. Decision No. 478/MON of 8 December 2014, areas divided in terms of the nature of the activity, where the function is only a staff process, and the capabilities are tools that can have an impact. It is a division adopted under NATO, resulting from its policies, military policies and doctrines. Decision 478 / MON lists one function – information operations – and three abilities – public diplomacy, social communication and psychological operations.

communication capabilities seems to be a desirable solution. Realizing the importance of the actions taken in the initial stage of staff training can definitely contribute to increasing the effectiveness of strategic communication. The understanding by the command level of the consequences of the actions taken, their impact on the information environment, may significantly affect the level of implementation of tasks within the armed forces, and, consequently, the perception of the Ministry of Defense in accordance with the political and military goals set in StratCom (NATO Military Policy On Strategic Communications, SH/SAG STC/AM/17-318278, 2017).

Neutral threats, e.g. in the form of a natural disaster, may also be an element used in the implementation of image-related strategic communication tasks. Therefore, the use of engineering troops or general military subunits in this particular case can definitely have a positive impact on the process of perceiving the ministry. Skilful use of soldiers as an element of strategic communication (communicated through actions taken) may affect the positive perception of not only the public opinion of the region affected by the natural disaster, but also show the public the willingness of the ministry to help the victims. Information noise can also be included in the category of neutral threats. Nowadays, it results from the universality and availability of all information channels in the space of the information dimension of the environment. Messages are created on an ongoing basis, distorted (intentionally or completely unconsciously), and then distributed for the purposes of communication with target groups. It often happened that the mainstream media, not knowing the proper conceptual apparatus, described the changes taking place in the armed forces. Both the structural and hardware changes have their supporters and opponents, so using the right wording is extremely important. Therefore, it seems important to be absolutely transparent towards journalists, and at the same time to educate them in the use of the appropriate conceptual apparatus during the work on the material for publication (NATO Military Policy On Strategic Communications, SH/SAG STC/AM/17-318278, 2017).

Image-related threats resulting from the actions of the opponent (potential opponent) constitute the broadest category. They concern deliberate communication activities, the intended effect of which is to reduce the credibility of the armed forces. Among hostile actions of this type, one should distinguish, first of all, propaganda and disinformation aimed at influencing political leaders in order to disrupt the decision-making process, influencing military commanders of various ranks in order to overpower the command system of armed forces, or influencing the society or social groups in the media to undermine the decision-making process. the credibility of the leaders or disrupting the functioning for the benefit of society. Therefore, it seems important to conduct analytical activities in the scope of defining the directions of threats and developing schemes to counteract them. It should also be borne in mind that many state entities, but also extremist groups (including those that use terrorist activities as an element of combat), currently operate within the information environment. Therefore, it is important that a potential threat (e.g. political, military, economic, social, information) is diagnosed at an early stage, which may help minimize the effects of a planned attack (NATO Strategic Communications Handbook, SH/STC/15-309090, 2015).

The above considerations in terms of image threats prove that not all threats may come from propaganda or disinformation activities carried out by hostile entities. The factor connecting these threats is the cognitive dimension of the information environment, where the activities undertaken by the ministry are discussed within various demographic groups.

As a result, judgments of decisions (actions) made by the ministry are formed, which in turn are the source of information in the publicly available space at a later stage. Of course, the information would not reach a potential recipient without the physical sphere, i.e. a network of tools with the help of which information is disseminated among selected audiences (e.g. press, radio, TV, social media, or even a peer-to-peer network within which information is reproduced).

The level of trust in the indicated institutions is a reflection of the image-building activities undertaken by national ministries. And so, according to CBOS, by September 2020, there had been fewer positive opinions about the functioning of the army. Currently, nearly seven out of ten respondents speak of it approvingly (69%, since March a decrease by 3 percentage points), while it is criticized by every twentieth (5%). Objections to the activities of the army are most often expressed by respondents who identify themselves with the left, who are not religiously engaged, as well as the youngest respondents (Komunikat z badań, 2020).

Table 1. Assessment of the military activity in the years 2011-2020

Oceny działalności wojska	Wskazania respondentów według terminów badań																			
	2011	20	12	20	13	20	14	20	15	20	16	20	17	20	118	20	119	20	20	Zmia
	IX	III	IX	III	IX	III	IX	III	IX	III	IX	III	IX	III	IX	III	IX	III	IX	'20
	w procentach												,20							
Dobra	65	66	69	55	66	66	67	62	69	66	69	60	65	59	64	73	74	72	69	-3
Zła	9	9	6	10	4	8	7	8	4	6	6	12	11	8	7	10	7	5	5	0
Trudno powiedzieć	26	25	25	35	30	26	26	30	27	28	25	28	24	33	29	17	19	23	26	+3

Source: (CBOS nr 121/2020).

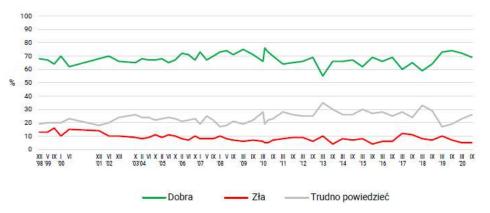


Figure 1. Assessment. Assessment of the military activity in the years 2011–2020 Source: (CBOS nr 121/2020).

In another CBOS study on the attitude towards various institutions and organizations of public life, the military (83%) and NATO (80%) also enjoy high public trust among the 20 entities mentioned.

Table 2. Trust in the social sphere in 2020 r.

	Czy, ogólnie rzecz biorąc, ma Pan(i) zaufanie czy też nie ma Pan(i) zaufania do wymienionych instytucji?										
Instytucje	Zdecydo- wanie mam zaufanie	Raczej mam zaufanie	Zaufanie – ogółem	Raczej nie mam zaufania	Zdecydo- wanie nie mam zaufania	Brak zaufania – ogółem	Trudno powie- dzieć				
	w procentach										
wośp	48	36	84	7	5	12	4				
Wojsko	28	55	83	5	3	8	9				
NATO	20	60	80	5	1	6	14				
Caritas	24	54	78	8	5	13	9				
PCK	20	57	77	6	2	8	15				
Władze lokalne	12	62	74	13	4	17	9				
Unia Europejska	14	59	73	12	5	17	10				
ONZ	16	56	72	7	2	9	19				
Policja	11	60	71	16	5	21	8				
Rzecznik Praw Obywatelskich	17	47	64	9	3	12	24				
Kościół rzymskokatolicki	22	42	64	21	11	32	4				
Urzędnicy administracji publicznej	4	57	61	18	5	23	16				
Prezydent	26	32	58	16	20	36	6				
Rząd	13	33	46	24	21	45	9				
Sądy	3	39	42	33	12	45	13				
Trybunał Konstytucyjny	7	33	40	21	16	37	23				
Związki zawodowe	3	31	34	20	7	27	39				
Sejm i Senat	2	31	33	36	9	45	22				
Media	2	30	32	37	18	55	13				
Partie polityczne	1	23	24	41	15	56	20				

Source: (CBOS nr 43/2020).

Compared to previous measurements, NATO gained public trust (an increase from 62% to 80% compared to $2016)^4$ and the military (from 79% to 83%) (Komunikat z badań "Zaufanie społeczne", nr 43/2020).

⁴ It is worth noting that the level of trust in NATO and the United Nations is the highest among those recorded so far.

Tak Nie Tp 10 11 10 10 17 11 76 63 83 83 84 76 59 82 78 83 15 60 23 22 60 18 6 63 29 75 19 79 17 4 78 38 50 53 33 42 47 45 47 40 13 56 32 39 51 10 59 29 11 45 44 45 37 27 27 32 37 31 34 29 20 30 24 16 39 44 15 28 54 17 18 21 68 14 76 11 10 33 68 23 55 34

Table 3. Trust in the social sphere in 2020 r.

13 18 62 15 24 55 21 24 60 16 24 63

Source: (CBOS nr 43/2020).

- 69

The strategic communication tool used against image threats are the activities of PSYOP, which, as Claes Wallenius and Sofia Nilsson write

troops by sending various types of demoralizing messages via leaflets. A further purpose directed towards specific and distinct groups is to influence or disrupt an opponent's decision-making processes. Related to this, is the concept of reflexive control, used primarily in the Russian military science theories. A third purpose is to influence public opinion in both domestic and foreign populations through a certain form of propaganda. In addition, the development in the Middle East has shown a new pattern of psychological terror aimed at intimidating opponents by posting brutally violent acts on the Internet (Wallenius, Nilsson, 2019).

4. CYBER THREATS

Cyber threats are usually equated with the actions of the enemy (potential opponent) on infrastructure elements (e.g. networks, workstations, servers, radio, television, etc.) serving as channels of communication with the public or directly on the critical infrastructure of the armed forces in order to disrupt the process. decision making (Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, 2014).

Disruption of communication channels reduces the effectiveness of the activities carried out. It may be carried out with the task of temporary or permanent damage to the network, ICT systems or devices through which communication is carried out both inside and outside the ministry. Effective infrastructure security must take into account maintaining appropriate security standards at all levels of command.

Therefore, an important element in the strategic communication system is the protection and defense of the state's cyber infrastructure. In addition, in the event of a cybernetic event,

^{*} W tabeli połączono odsetki odpowiedzi zdecydowanie mam zaufanie i naczej mam zaufanie oraz zdecydowanie nie mam zaufania i raczej nie mam zaufania. Na szarym tle zaznaczono odsetki wskazniace na przewana deklaracii wzraż siarzono zaufania.

when an external deliberate activity causes information chaos, there is also a probability of interference in the form of information noise. This can translate into a temporary lack of a coherent message, which is crucial in the case of StratCom. Therefore, in addition to the protection of sensitive infrastructure, attention should be paid to the knowledge of the current lines of narrative of the Ministry of Defense, including topics to be emphasized / avoided as part of conducting activities (including communication) in accordance with the competences held (NATO Military Policy On Strategic Communications, SH/SAG STC/AM/17-318278, 2017).

The most common goal of activities in cyberspace is to disrupt the decision-making process of an institution. If there is no unanimity in making a decision, or if it is not possible to send the task to be carried out by subordinate elements, there may be decision chaos, which in turn may contribute to an image problem. In addition, a case not related to the chain of command but with the effect of disrupting official channels of communication with the public as part of wider strategic communication, i.e. hijacking a social profile (e.g. Twitter, Facebook, etc.). The control over the electronic media taken over may both negatively affect the image of the institution, but also become a tool for the manipulation of an entity hostile to the ministry. In addition, in the discussed case, there is a risk of stealing sensitive data remaining within the ICT systems, which can be used to impersonate these persons. One must take into account the likelihood of information warfare activities aimed at using the obtained data to undermine the competence of high-ranking government officials.

A tool that has many advantages but also creates many threats are social media, i.e. channels for direct communication, expressing thoughts and judgments. Protecting yourself in the event of hostile influence, the use of social engineering or social engineering is very difficult, but not impossible. Users must be aware of the threats resulting from disinformation and propaganda activities by entities hostile to actions taken at the state level, including the level of the Ministry of Defense.

An important problem in cyber threats is the attribution of the attack. In the twenty-first century, there are many techniques and tools supporting the process of hiding the sources of devices indicating the place from which the attack was made. It should be taken into account that as part of the arms race, a potential enemy will try to direct his actions to another area in order to mask operational ones (e.g. using a global network of connections, a network of nodes allowing anonymous access to resources, impersonating public figures, e.t.c.) (NATO Military Policy On Strategic Communications, SH/SAG STC/AM/17-318278, 2017).

Research in the field of cyber network security is undertaken by numerous research centers, however, as noted by Jha, A.V., Appasani, B., Ghazali, A.N.

according to the Scopus database, the statistics for the year-wise research articles published in the context of the CPS cyber networks are illustrated in Fig. 1. It can be observed that research has been focused on addressing the security and safety issues in CPS. However, not much research has been found on the reliability of the cyber networks (Jha, Appasani, Ghazali, Pattanayak, Gurjar, Kabalci, Mohanta, 2021).

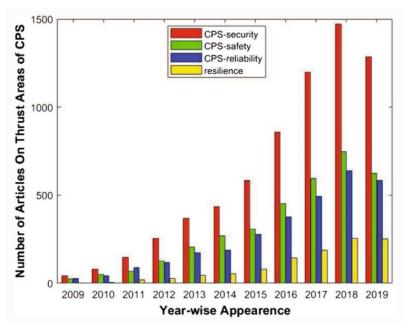


Figure 2. Publication statistics on cyber networks Source: (Appasani, Ghazali, Pattanayak, Gurjar, Kabalci, Mohanta, 2021).

5. MILITARY THREATS

Military threats are a category of threats to the information environment that occur in wartime or in the course of an operation (Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014). The main goal of this type of threat is to disrupt the decision-making process of the operation commander or commanders subordinate to him, as well as lowering the morale of troops and the will to fight. The main method of operation is to sabotage information, communication and reconnaissance systems. In addition, one should take into account the direct and indirect destruction of resources through a lethal effect on the technical elements of the command and communication system, as well as attempts to overpower the command and control system of subordinate troops. It should also be understood that actions consisting in destroying, overpowering, harassing or demolishing will carry a specific message that will affect not only the physical dimension of the information environment. The use of conventional forces, the destruction of state infrastructure, or terrorist attacks carried out by ideological fanatics will carry a message that will also have a significant impact on the cognitive dimension of the information environment. A society exposed to direct attacks will be subject to psychological pressure, which in turn may have an impact on reevaluating personal goals as well as expressing opinions and concerns about the competence and ability of forces and means to defend themselves (NATO Military Policy On Strategic Communications, SH/SAG STC/AM/17-318278, 2017).

There is a relationship between communication technology and political conflicts and violence. Nils B Weidmann writes that

there are different pathways through which this can happen: technology can facilitate collective action, but at the same time give governments the opportunity to censor content and gather intelligence about dissidents. Also, audience effects can be introduced by the rich and instant transmission of information from conflict regions (Weidmann, 2015).

A special case of war threats in the information environment are the so-called phase zero, i.e. events occurring when the full spectrum of communication activities resulting from legal and ethical limitations regarding the use of forces and means of the destruction system in peacetime cannot be used. We can deal with such a situation when the opponent carries out offensive communication activities already in peacetime, with the intention of weakening the state's capabilities in the field of public diplomacy, the implementation of tasks by ministries, including the implementation of military strategic communication tasks. The threats may include attempts to undermine the legitimacy of the actions taken, discredit forces and resources within the national defense system, impersonating state officials, conducting disinformation and propaganda activities, as well as manipulating information (NATO Strategic Communications Handbook, SH/STC/15-309090, 2015).

As noted by Jha, A.V., Appasani, B., Ghazali, A.N.

another important challenge in this direction is the integration of traditional information technology (IT) systems with operational technology (OT) systems. OT systems differ from traditional IT systems with respect to the target, purpose, computing components, communication technologies, and interfaces as well as ownership and management (Jha, Appasani, Ghazali, Pattanayak, Gurjar, Kabalci, Mohanta, 2021).

REFERENCES

Hallahan, K., Holtzhausen, D., Ruler, B., Verčič, D., Sriramesh, K. (2020). Defining Strategic Communication. "International Journal of Strategic Communication", 1. DOI: 10.1080/ 15531180701285244.

Jha, A. V., Appasani, B., Ghazali, A. N., Pattanayak, P., Gurjar, D. S., Kabalci, E., Mohanta, D. K. (2021), Smart grid cyber-physical systems: communication technologies, standards and challenges. "Wireless Networks". DOI: 10.1007/s11276-021-02579-1.

Komunikat z badań "Oceny działalności instytucji publicznych" (2020). Warszawa: Centrum Badania Opinii Społecznej, nr 121/2020 (F. Feliksiak).

Komunikat z badań "Zaufanie społeczne" (2020). Warszawa: Centrum Badania Opinii Społecznej, nr 43/2020 (opr. Małgorzata Omyła-Rudzka).

NATO Military Policy On Strategic Communications, SH/SAG STC/AM/17-318278 (2017).

NATO Strategic Communications Handbook, SH/STC/15-309090 (2015).

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2014). Warszawa.

Wallenius, C., Nilsson, S. A. (2019). Lack of Effect Studies and of Effects: The Use of Strategic Communication in the Military Domain. "International Journal of Strategic Communication", 13:5. DOI: 10.1080/1553118X.2019.1630413.

Weidmann, N. B. (2015). Communication, technology, and political conflict: Introduction to the special issue. "Journal of Peace Research", 52:3. DOI: 10.1177/0022343314559081.

Zerfass A., Verčič, Nothhaft, H., Werder, K. P. (2018). Strategic Communication: Defining the Field and its Contribution to Research and Practice. "International Journal of Strategic Communication", 12:4. DOI: 10.1080/1553118X.2018.1493485v.

DOI: 10.7862/rz.2021.hss.31

The text was submitted to the editorial office: December 2021. The text was accepted for publication: December 2021.