ACTA UNIVERSITATIS WRATISLAVIENSIS
No 3903

Studia nad Autorytaryzmem i Totalitaryzmem 41, nr 1
Wrocław 2019

DOI: 10.19195/2300-7249.41.1.5

TOMASZ DUKIEWICZ
ORCID: 0000-0001-7833-9619
Uniwersytet Opolski

Information in the aspect of security threats and challenges

> Disinformation appears as a program aimed at replacing certain content recognized by the misinforming authority as inappropriate with other that it considers to be right in the consciousness, and above all, in the subconscious of the target population.
>
> Vladimir Volkoff,
> *Dezinformacja — oręż wojny*

Introduction

Information management can be defined as an information and decision-making process supported by the functions of organization planning and control, the purpose of which is to predict and solve problems of the state's operations with particular emphasis on the surroundings. Information management significantly reduces and eliminates threats that arise directly from the internal or external environment of the state.

Receiving information provides the recipient with the opportunity to broaden the message with the spectrum he is interested in, having a positive, neutral or negative impact on the interaction. Thus, messages can include a certain amount of information, so different messages should consist of different amounts of information about the same issue. On the other hand, if the information is received by two or more recipients, there is a risk of over-interpretation or manipulation through far-reaching similarity of the information which can be read by recipients as identical and constitute disinformation activities. Differences in the reception (reading) of the information may result from several factors:

— forms of the information transfer;
— subjective interpretation, reading of information;
— method of the information transfer.

The same messages can be transmitted in different forms, having the same features, properties and parameters, which may decide about relatively smaller or larger amount of the information they contain.

1. The value of information

A number of authors of studies in the field of this subject link the amount of information with the concept of probability. This theory finds the information as a "measure of the uncertainty of a certain event occurring (receiving a specific measurement result, a specific message emitted by the source) out of a finite set of possible events".[1] Developing this encyclopaedic formulation, it can be stated that the amount of the information contained in a given signal depends on the amount of the set of all signals concerning the information we are interested in. The dependence of the amount of the information on the size of the set will then be directly proportional. The larger the set of signals, the greater the amount of information, because there is less probability of a given character appearing in a specific context, and conversely, the less uncertainty the signal removes, the less information it brings.

Anyone interested in acquiring information will strive to obtain perfect information. In reality, however, and due to, among others, imperfections in the flow of information, it will not be possible. Therefore, in most cases we are dealing with information that is not perfect. The imperfection of information can relate to its three features: adequacy, timeliness and accuracy. One can therefore distinguish between inadequate information, outdated information and inaccurate information by characterizing the value of information as being imperfect.

Inadequate information is what we colloquially refer to as "off the subject", that is, having data on a different feature of the state of the object we are interested in than the desired one. We will define outdated information if we have received information about the value of the object's feature we are interested in, but concerning the past period.

Inaccurate information occurs when the value of the feature of the object we are interested in is overestimated or underestimated, that is, it does not correspond to the actual state of affairs.[2]

The military environment prioritizes the value of information which from the point of view of its recipient is understood as useful, current, complete and

[1] *Nowa encyklopedia powszechna PWN*, vol. 3, Warszawa 1998, p. 54.
[2] S. Forlicz, *Informacja w biznesie*, Warszawa 2008, pp. 23–24.

consistent content used both during the planning phase of the decision-making process as well as when commanding and heading the fight in the course of the operations carried out.[3]

An important place in the consideration of information is the measurement of information and the fundamental question: is it possible, and if so, how to measure information? We know that information can be measured accurately. The unit of information quantity is bit (bit is a piece). It has been assumed that the message, whose probability is p, contains:

$$k = log_2 \frac{1}{p} = -log_2 p \tag{1}$$

For example, if the source emits only one message, the probability of emission is $p = 1$, that is, this message carries $k = \log_2 (1) = 0$ information bits. This means that the message emission is certain, which at the same time implies a zero value of information in a given message. The situation changes when $p = ½, ¼$, etc., assuming that the source can transmit n different messages with the probability p_i, $i = 1, 2, 3, \ldots, n$, then the weighted average amount of information in messages from this source is:

$$H = \sum_{i=1}^{n} p_i \, log_2 \, \frac{1}{p_i} \tag{2}$$

The size of H is called the information entropy of the information source and comes from Claude E. Shannon, an American mathematician and engineer. Entropy is a weighted average of the amount of information that a single message transmits from an information source. Weights are the probabilities of sending individual messages by a given source of information. The unit of entropy is a bit (hence the base of the logarithm is 2). On the basis of the entropy value for a particular message, one can speak about the probability relation of occurrence of a given event to the amount of information contained in a message about a given event. This means that the less likely the result of a given event is, the more information there is about its occurrence.[4]

Information may have a zero value, so it will be useless for its holder when he has no means to use it. Information that provides knowledge about a certain state of affairs will be useless if it is not possible to apply it in future actions, therefore it will not influence the reality shaped by the potential user.

[3] *Regulamin działań wojsk lądowych*, Warszawa 2008, s. 309.

[4] T. Dukiewicz, H. Spustek, "Analiza i wartościowanie informacji w procesie decyzyjnym" [Analysis and valuation information in decision-making process], *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie* 2016, no. 92, p. 31.

The value of information depends on the factors listed below[5]:

— The quality of information which depends on its accuracy. The higher the quality of information, the greater the confidence of the commanders in relying on it during the decision-making process. At the same time, as the quality of information increases, its cost increases as well. For that reason, if the information, despite its high quality, cannot significantly contribute to the ability of making decisions, it is not worth incurring additional costs.

— The timeliness of information that should ensure that the information is provided through the information system to the right person at the right time, enabling decision-makers to take actions at the right time, thus preventing delays and missed opportunities.

— The amount of information as only the right amount of information can ensure that the right decisions are made. Both scarcity and excess of the information may lead to a decrease in the effectiveness of the decisions made. A decision-maker in the flow of information may overlook information that is the most important or key at the moment to accomplish goals of the organization.

— The relevance of information which means that the information that reaches the decision-makers should be linked to tasks they have to complete.

Information is the main element of disinformation through the imperfection of information and, as a result, its negative impact on various spheres of the security and the functioning of society.

2. Information as the main element of disinformation

The official EU definition of disinformation was developed by a team of experts from EU member states under the guidance of Professor Madeleine de Cock Buning from the University of Utrecht.

According to the definition of the EU directive, disinformation is understood as "false, inaccurate or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".[6] Disinformation can be detrimental to democratic processes, values and can be deliberately directed to affect a wide range of areas such as security issues, science, education or finance.

According to a NATO directive, disinformation is "any undertaking aimed at misleading an opponent by manipulating, pretending to act and fabricating evidence that provoke actions detrimental to his own interests".[7] Disinformation is also a typical information activity involving the manipulation of the message and

[5] J.A.F. Stoner, R.E. Freeman, D.R. Gilbert, *Kierowanie*, transl. A. Ehrlich, Warszawa 1999, pp. 589–590.

[6] https://ec.europa.eu/digital-single-market/en/fake-news-disinformation (accessed: 24.01.2019).

[7] http://cepa.ecms.pl/files/?id_plik=2773 (accessed: 7.12.2018).

the use of lies, the purpose of which is to create a message beneficial to the country that uses it.

In the aspect of messages provided using social media, it is automated and often based on the dissemination of false information. According to a Robotrolling report by NATO STRATCOM, 50% of all accounts tweeting about NATO in the Russian space are bots (false information). The English-speaking space contains 40% of Twitter accounts.[8]

Sir Julian King stated that information attacks are another category of interference in the social and political situation of the country. For that reason, the challenges of manipulation and influencing citizens' behavior should be treated differently to standard cyber threats. As he added, "the informational impacts may come from many sides, but we should say directly that they also come from Russia".[9]

The most powerful global player using described methods and means of influence without scruples is Russia, which has recently been repeatedly identified as the perpetrator of abuses associated with influencing the electoral processes. Its main motive is to sow discord in Western societies in order to weaken the European and Transatlantic community, which is considered as the main rival of Russia.

Political campaigns, which are by their nature a period of increased tensions in societies, are an opportunity to use such disinformation techniques to deepen divisions. Simultaneously, they provide opportunities to strengthen political forces, groups and individuals whose active operations are conducive to Russia's strategic objectives, and at the same time to weaken those that Moscow considers to be detrimental to its interests in a given country or region. The most spectacular example of such interference was a large-scale operation supporting organizations in favor of UK's exit from the EU during the campaign before the Brexit referendum in 2016. The same model of actions was adopted by Russia during events regarding the so-called referendum on the independence of Catalonia held on 1 October 2017.

Russian influence can be exerted in numerous aspects:

— enabling implementation of Russia's strategic objectives;

— hindering political decision-making process contrary to the interest of the Russian Federation;

— inspiring and fuelling tensions between Western countries, mainly NATO;

— maintaining the possibility of applying military pressure in Central, Eastern and Northern Europe;

— maintaining a dominant position as an energy supplier to Europe;

[8] https://www.stratcomcoe.org/report-russian-language-twitter-conversation-about-nato-dirty-dynamic-and-deceptive (accessed: 20.06.2018).

[9] https://www.theguardian.com/world/2018/jun/20/britains-top-eu-commissioner-lays-out-proposal-to-tackle-disinformation (accessed: 20.06.2018).

— struggling to maintain Russia's position as a decision-maker in terms of world peace;

— promoting the thesis about the moral right of Russia to influence the fate of other nations;

— conducting protective actions in crisis situations for Russia;

— maintaining the ability to influence public opinion in other countries.

Actors involved in disseminating disinformation include:

— intelligence services of Russia;

— collaborators of the intelligence of Russia;

— hackers inspired and controlled by the Kremlin;

— political allies of Moscow;

— influence agencies;

— scientists, experts, cultural personalities, journalists;

— Russian companies or owners of international economic corporations;

— non-governmental entities;

— unaware disinformers;

— Russian and pro-Russian media.

In Poland, defence policy should be regarded as a fertile ground for the informational influence by diminishing the importance of the Polish army, undermining faith in NATO allies. The impact through informational operations is usually targeted at the state's strategic pillars, including energy security, and in particular projects for the construction of Polish energy independence. Regional cooperation is also under attack and escalation of tensions in Poland's relations with its neighbors is provoked. The aim is also the image of Poland in respect of its impact on Europe and NATO, as well as weakening the importance of the Visegrad Group through individual policies in relation to each of these countries.

The results of the literature analysis indicate that direct psychological impact is identified with disinformation, especially those actions which are addressed directly to the headcount.

Based on the assumption that disinformation is misleading by providing false (misleading) information, direct psychological impact can therefore potentially be one of the main elements misleading soldiers and the population of the potential country or the real opponent, especially its national minority. Disinformation will be the influence of the subject of actions on the army and the population of the opponent, which based on the transfer of false data will lead to drawing certain conclusions and beliefs that are desirable for the purpose of the actions carried out. The goal of psychological actions is to implement a consistent program aimed at changing in the consciousness of the subject those interactions of views which are considered to be unfavorable for the forces conducting the operation. When Aleksandr Solzhenitsyn described the gloomy reality of the USSR, and especially the way of treating people with different political views and questioning the power of the Soviet empire, he broke off an intricately prepared disinformation

program.[10] In retaliation, the Soviet authorities took a number of disinformation measures which discredited both the attitude and achievements of the author of the novel. In a memorandum to the Council of Ministers dated 4 January 1976, Andropow, the head of the KGB, wrote with satisfaction about "dropped interest in Solzhenitsyn abroad and in the USSR". He also admitted in the same document that the KGB, through their agents and various contacts, helped spread in the West "materials useful for us" that discredited Solzhenitsyn and his "class hatred of the Soviet authorities".[11] This example is an argument to justify the thesis that disinformation is also part of psychological activities aimed at changing the way of thinking and perceiving.

3. Models of data transfer for spreading disinformation

Based on the source literature it can be concluded that the subject of actions can use two models of data transfer for spreading disinformation. The first one is a reflecting–deflecting model in which the subject of actions uses a false source of information transfer, which makes it completely unknown to the object of interactions. The second model — legitimate — boils down in its essence to transferring the responsibility for disseminated information. According to this practice, the subject of actions wants to hide his authorship of the prepared message and sends it first to a substitute broadcaster, then gets from this broadcaster his "own" message and sends to the object of interactions as obtained from a foreign source of information. Using this method, information can be transferred which at the given moment cannot be reliable as it comes from the source of unknown origin.[12] According to Michal Koudelka, head of the Security Information Service (BIS, counterintelligence), espionage activity in the Czech Republic is currently focused on small information from the state institutions and authorities. China and Russia have the largest secret agent base there. Seemingly insignificant information from specific industries or environments is now priority for foreign intelligence.

The construction of nuclear power plants can serve as an example. A foreign power treats secret plans concerning their erection as equally important as information about people who make decisions related to those plants or the conditions in which they will be built. This is also the way we should look at the fact that as soon as the Czech government examined the issue of building new nuclear power plants in 2018, a secret meeting took place in Moscow between the president's adviser and businessman Martin Nejedlý and the CEO of Rosatom Alexei Lichaczow, whose company can win the contract. Politicians and public officials are particularly ex-

[10] A. Sołżenicyn, *Archipelag Gułag*, transl. J. Pomianowski, M. Kaniowski, Warszawa 1990.

[11] D. Remnick, *Zmartwychwstanie*, transl. M. Słysz, Warszawa 1997, p. 138.

[12] D. Kosárová, "Information warfare and the contemporary security environment", *Horyzonty Bezpieczeństwa* 8, 2017, no. 3, pp. 18–19.

posed to such actions. However, a particular object of interest are journalists with accreditation and access to places and people that ordinary citizens do not have. As emphasised by Koudelka, contemporary espionage is primarily about getting closer to and influencing decision-making processes, and thus the functioning of the state, which is more valuable than secret documents.[13] Such activities carried out by secret intelligence are coordinated with hybrid and informational operations. In the opinion of Koudelka, one of the best examples of large-scale hostile information in the Czech Republic was a disinformation campaign on the construction of an element of the American anti-missile shield, that is, a radar at the military base in Brdy.[14] Particularly noteworthy is the moment of discussion on the theoretical possibilities of locating the US missile base in the Czech territory. Hostile actions in that case have accomplished their goal. There has been a great deal of disinformation content, half-truths and conspiracy theories which divided the debate. Such actions exerted great pressure on media and political elites. As highlighted by Koudelka, many politicians have changed their minds on this subject. The outcome of these actions was establishing a special department within the Ministry of the Interior whose task was to combat such activities. In Koudelka's opinion, the state in such a situation can only use the same weapon, that is, information.[15] It has to be concrete, clear, easy to understand and coordinated in time. In turn, the responsibility of the domestic intelligence is to communicate and present the truth about the importance and necessity of cooperation within the EU and NATO in the context of increased security threats and challenges.

Further analysis of the source literature makes it possible to separate two general limitations in the aspect of the use of disinformation:

— Disinformation can only be used if there is a certain group of soldiers or opponent's population already confused or vulnerable to the information influence.

— Disinformation can potentially increase the level of dissatisfaction with the situation in the enemy's troops and its society, but it will be effective only if it takes advantage of existing hotspots (e.g., supply problems, poor level of technical equipment). It is therefore pointless to mislead the public by providing information which not only does not cause confusion, but may even raise objections and doubts as to the reliability of the source.

The above restrictions result directly from the specifics of disinformation interactions which in their essence consist not in the fact that the object believes in something suggested by the subject, but in modifying his attitudes and behaviors.

[13] https://www.cyberdefence24.pl/szef-kontrwywiadu-czech-o-zagrozeniu-dezinformacja-i-szpiegostwem-z-rosji-i-chrl (accessed: 22.04.2018).

[14] Ibid.

[15] Ibid.

As a result, it can be stated that two techniques can be included in the personal disinformation forms: simulation and manipulation.[16]

Simulation consists in the artificial creation of an "image" (object, activity, etc.) close to the real one. The purpose of apparent actions is to lie to the opponent, that is, to mislead him. Apparent actions should be defined as a complex of organizational, material and practical measures consistent with the objective and tasks of the operation, place, time and manner of operation of the troops, aimed at deceiving the opponent as to the actual intention of fighting forces, their composition, conditions, real tasks in the course of preparation and carrying out operations. Apparent action is any activity that indirectly affects the opponent. It determines the results of his personal identification as the main source of data. Therefore, if they are found to be true, they will make the opponent's decisions wrong.[17]

The second form of personal disinformation in psychological activities is manipulation. The concept of manipulation is ambiguous and not easy to define. The attempts to organize knowledge in this field, including the aspects of social psychology, sociology and social engineering made so far have not given clear results. When dealing with the issues of manipulation, it is often precisely the instrumental approach that seems appropriate for this type of activities, given the tasks that the subject of these interactions carries out and the relationships that exist between the subject and the object of these activities. In order to understand the essence of manipulation, it seems advisable to consider the analyzed concept in the context of social impact and persuasive influence on human attitude and behavior. Each member of the community directly or indirectly involved in the armed struggle is subject to a certain social impact, reacts to the environment and tries to shape his surroundings. For that reason, manipulation makes use of feelings and emotions. Providing fake information, taking into account that these activities are carried out in a dense social environment, while the individual suffers from information scarcity, it can therefore be found that the transferred content has the ability to trigger a number of emotions and feelings in the object of influence in order to provoke specified functional and verbal behaviors.[18] In this case, disinformation will permanently strive to limit or completely block control mechanisms of consciousness of the individual on whom it intends to impose assumed patterns of attitudes and behaviors.

[16] T. Dukiewicz, "Information operations", [in:] *Security Forum 2016: Volume of Scientific Papers*, ed. J. Ušiak, Banska Bystrica 2016, pp. 49.

[17] M. Wrzosek, *Dezinformacja jako komponent operacji informacyjnych*, Warszawa 2005, pp. 106–107.

[18] I. Pikner, V. Galatík, "The use of the armed forces in the postmodern wars", [in:] *The 21st International Scientific Conference "Knowledge-Based Organization": Management and Military Sciences*, Sibiu 2015, pp. 90–93.

Conclusions

Information in the security system is a driving force that brings together all tasks, security threats and the time required for accomplishing the objectives of actions into its common whole. Existing systems in the field of security management should be resistant to disinformation and information operations. There is no room for the freedom of interpretation of the information acquired since every decision results in the actions of people, therefore it requires accuracy and caution. This issue takes on a special dimension when it concerns the state, because this environment contains specific features such as a changing environment, time scarcity and often verified information. Only efficient management of information processes can have a positive impact on the development and elimination of the state threats. As a result of the dynamic development of technical possibilities for information transfer, and therefore also its electronic processing and modification, the catalogue of tools and circumstances where disinformation is used is growing. For that reason, one cannot forget about constant improvement of techniques and methods of disinformation. Building social resilience can play an important role in disinformation prevention. Social resilience stands against threats and challenges concerning the way the information is interpreted and analyzed. Actions involving psychological or informational influence may also be carried out by other entities, state-owned, non-state and private, including those located on their own territory. First and foremost, our security depends on ourselves, and by taking it into special consideration, we also increase the state's resilience to internal and external threats.

Bibliography

Dukiewicz T., "Information as a determinant of a decision system", [in:] *Proceedings of the International Scientific Conference of Business Economics, Management and Marketing 2018*, eds. P. Mikuš, M. Cenek, Masaryk University 2018.

Dukiewicz T., "Information operations", [in:] *Security Forum 2016: Volume of Scientific Papers*, ed. J. Ušiak, Banska Bystrica 2016.

Dukiewicz T., Spustek H., "Analiza i wartościowanie informacji w procesie decyzyjnym" [Analysis and valuation information in decision-making process], *Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie* 2016, no. 92.

Forlicz S., *Informacja w biznesie*, Warszawa 2008.

http://cepa.ecms.pl/files/?id_plik=2773 (accessed: 7.12.2018).

https://www.cyberdefence24.pl/szef-kontrwywiadu-czech-o-zagrozeniu-dezinformacja-i-szpiegostwem-z-rosji-i-chrl (accessed: 22.04.2018).

https://ec.europa.eu/digital-single-market/en/fake-news-disinformation (accessed: 24.01.2019).

https://www.stratcomcoe.org/report-russian-language-twitter-conversation-about-nato-dirty-dynamic-and-deceptive (accessed: 20.06.2018).

https://www.theguardian.com/world/2018/jun/20/britains-top-eu-commissioner-lays-out-proposal-to-tackle-disinformation (accessed: 20.06.2018).
Kosárová D., "Information warfare and the contemporary security environment", *Horyzonty Bezpieczeństwa* 8, 2017, no. 3.
Nowa encyklopedia powszechna PWN, vol. 3, Warszawa 1998.
Oulehlová A., Malachová H., Svoboda O., Urbánek J., "Preparedness of critical infrastructure subjects in energy sector for crisis situations", [in:] *Safety and Reliability of Complex Engineered Systems*, ed. L. Podofilini et al., London 2015.
Pikner I., Galatík V., "The use of the armed forces in the postmodern wars", [in:] *The 21st International Scientific Conference "Knowledge-Based Organization": Management and Military Sciences*, Sibiu 2015.
Regulamin działań wojsk lądowych, Warszawa 2008.
Remnick D., *Zmartwychwstanie*, transl. M. Słysz, Warszawa 1997.
Sienkiewicz P., "Information engineering problems", [in:] Materials from the scientific symposium, Warsaw 2002.
Sołżenicyn A., *Archipelag Gułag*, transl. J. Pomianowski, M. Kaniowski, Warszawa 1990.
Stoner J.A.F., Freeman R.E., Gilbert D.R., *Kierowanie*, transl. A. Ehrlich, Warszawa 1999.
Wrzosek M., *Dezinformacja jako komponent operacji informacyjnych*, Warszawa 2005.

INFORMATION IN THE ASPECT OF SECURITY THREATS AND CHALLENGES

Summary

In the article, the author describes the driving force behind deliberate informational activities. He pays particular attention to the current security situation in the information dimension. Existing systems in the area of security management should be resistant to disinformation and informational operations. There is no room for the freedom of interpretation of the information acquired since every decision results in the actions of people, therefore it requires accuracy and caution. This issue takes on a special dimension when it concerns the state, because this environment contains specific features such as a changing environment, time scarcity and often verified information. Only efficient management of information processes can have a positive impact on the development and elimination of state threats. Actions involving psychological or informational influence may also be carried out by other entities, state-owned, non-state and private, including those located on their own territory. First and foremost, our security depends on ourselves and by taking it into special consideration we also increase the state's resilience to internal and external threats.

Keywords: information, information processing, disinformation, security system, national security.

Tomasz Dukiewicz
tdukiewicz@uni.opole.pl