SECURITY DIMENSIONS
NO. 33; 2020 (150–165)
DOI DOI 10.5604/01.3001.0014.2675

The Concept of Information Metabolism by Antoni Kępiński and the Mechanism of Information Manipulation. Conditions for Effectiveness and Ways of Counteraction

Tomasz Aleksandrowicz[1]

ABSTRACT

In the modern security environment, information warfare is an increasingly important threat. The purpose of this article is to determine the conditions for the effective achievement of political objectives through the manipulation of information and disinformation. The conducted research used system analysis, also using case studies, generalizations and synthesis. This allowed to state that the key condition for the effectiveness of conducted information attacks is the mechanism described in the works of Antoni Kępiński as information metabolism. This makes it possible to formulate a postulate on the need to counteract such attacks based on building defensive and offensive capabilities of the state in the sphere of information warfare.

[1] Assoc. Prof. Tomasz Aleksandrowicz, Ph.D., Police Academy in Szczytno, Szczytno, Poland; correspondence address: Marszałka Józefa Piłsudskiego 111, 12-100 Szczytno, Poland; email: t.aleksandrowicz@wspol.edu.pl

ARTICLE INFO

Article history
Received: 31.01.2020 Accepted: 5.06.2020

Keywords
information warfare, information metabolism, disinformation, reflexive control

Introduction

Information has always been an important part of security environment. Its importance has significantly increased in the information society, whose features enable the use of disinformation and manipulation of information on a mass scale. The aim of this article is to establish a mechanism that allows for such manipulation of information that encourages its recipient (the target of an information attack) to take action and behave in a way consistent with the attacker's interests. The key element of this process is the mechanism of information metabolism which is the basis of the concept developed by Antoni Kępiński.

Characteristics of the modern infosphere

The term *infosphere* has already gained wide recognition in science and official documents. It is usually used as a synonym for *information space or information environment*. At first, it was used primarily in information science, but it quickly found its place also in security sciences.[2] The dominant opinion among researchers is that infosphere should be understood as all information resources to which a given entity has access. The importance of infosphere has definitely increased with the dynamic development of information society, which was directly related to the technological revolution in information acquisition, collection, processing and transmission. From the viewpoint of national security, this means that the state has become dependent on an efficient, fast, and loss-free circulation of information (just

[2] See also: B. Sosińska-Kalata, *Obszary badań współczesnej informatologii (nauki o informacji)*, "Zagadnienia Informacji Naukowej", 2013, no. 51, pp. 9–41; M. Kisilowska, *Przestrzeń informacyjna jako termin informatologiczny*, „Zagadnienia Informacji Naukowej", 2011, no. 2, pp. 35–52.

as it has become dependent on access to electricity in the 20th century), and the state's information resources, which must be protected, are targets for the opponent's attack. The potential opponent may introduce such information into the local infosphere that will serve to weaken the state and its society, and thus lead to information warfare. Infosphere must therefore be seen as a security environment of the state with opportunities, challenges, threats and risks. The importance of this issue will grow in the foreseeable future, if only due to the development of information technologies.[3]

From the viewpoint of state information security[4], one can distinguish several characteristics of modern infosphere. First of all, access to information is almost universal in the information society, which results in growing difficulties in maintaining the confidentiality of information and data, including personal data. Information protected by the state is increasingly becoming – despite actions taken to maintain its confidential nature – public property. On the other hand, we are dealing with the freedom to publish and reproduce information on a global scale. Such possibilities are in the hands of individuals who can easily make a piece of information public, for example through social media networks. The network environment is characterised by a cascade effect which means that information shared by a single user of Twitter, or of another social networking site, can be duplicated by *x* other users, and the entry of each user can be then duplicated by *y* other users without any limitations; the process can go on forever. This is facilitated by the multiplicity of information channels with a potentially global reach, which enhances not only access to the information, but also its reproduction and distribution.

There are two fundamental consequences of this situation. First of all, the amount of information available on a global scale has already exceeded the threshold of so-called *attention crash* – the moment when the information one wants to assimilate exceeds one's ability to focus attention. The amount of data is growing more rapidly than the human brain's ability to process

[3] See: T. Aleksandrowicz, *Infosfera jako środowisko bezpieczeństwa państwa. Próba konceptualizacji problemu*, [in:] *Nauka i praktyka bezpieczeństwa. Księga pamiątkowa Leszka Fryderyka Korzeniowskiego, profesora Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie*, A. Kozera, E. Sadowska (eds), Kraków 2019, p. 308 *et seq.*

[4] More information on the concept of state information security can be found in: T. Aleksandrowicz, *Bezpieczeństwo informacyjne państwa*, „Studia Politologiczne", 2018, no. 49, pp. 33–50.

it. Gleick calls this factor the *devil of information overload*.[5] Therefore, it is increasingly difficult to assess not only the importance of information, but also its truthfulness and actual significance for the recipient. This creates a space for various types of information manipulation; not only may the recipient miss the piece of information that is of significance to him/her, but also some information may be intentionally exposed and others may be underestimated, which depends on the sender. Such a situation was described in 2015 by Eco: "when we want to give our opinions in secret, we also have other means at our disposal. In order to know what the newspaper is supposed to contain, you need to, as the editors say, define the agenda. There are many news to inform the readers about, but why should we say that there was an accident in Bergamo and not say that there was another accident in Messina? It is not the news that makes the newspaper, it is the newspaper that makes the news. By skilfully compiling four different news, the reader is offered another one".[6]

Second of all, as Madej notes, "the concept of information revolution refers to a kind of a social megatrend in the modern world, manifested by growing possibilities of media influence, especially mass media, on the course of political and social processes, instead of on technological changes, which make it possible to increase the importance of information".[7] This can be clearly seen when looking at changes in the nature of conflicts: while the goal in the classical form was the opponent's armed forces and defeating them on the battlefield, in modern conflicts the goal usually concerns the opponent's (society's) awareness, and victory is achieved through disorganisation of the political, economic or – last but not least – information systems.[8] It should be noted that the instruments enabling such actions

[5] J. Gleick, *The Information. A Theory. A History. A Flood*, New York 2011, p. 11. Cf.: T. Aleksandrowicz, *Świat w sieci. Państwa. Społeczeństwa. Ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, 2nd edition, Warszawa 2018, p. 65 *et seq.*

[6] U. Eco, *Temat na pierwszą stronę*, Warszawa 2015, translation: publisher.

[7] M. Madej, *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [in:] *Bezpieczeństwo teleinformatyczne państwa*, Madej M., Terlikowski M. (eds), Warszawa 2009, p. 18, translation: publisher.

[8] See T. Aleksandrowicz, *Wojna jako narzędzie polityki w XXI wieku. Stare pojęcia – nowe konotacje*, [in:] *Siła we współczesnych stosunkach międzynarodowych*, W. Kostecki, K. Smogorzewski (eds), Warszawa 2017, p. 85 *et seq.*

are not only at the exclusive disposal of states; they are also available to non-state entities.

Practical use of the mechanism of information metabolism

The concept of *information metabolism* was developed by a Polish psychiatrist Antoni Kępiński. As Kępiński notes, information metabolism consists of two phases. In the first phase, a person strives to gain orientation in the external world in order to limit the created models of reality and to make decisions about his/her own actions. In the second phase, the person takes action on the basis of the chosen model and receives information about his/her own activity. Thus a feedback loop is created: receiving information about the surrounding reality – creating a model of reality – acting – acquiring information about one's actions.[9]

In practice, this means that by perceiving reality, a person creates its model (or, by definition, simplification) and on that basis he/she makes decisions. If the perception of reality is in any way disturbed – whether by external factors or as a result of the observer himself/herself – the model he/she creates, and thus the decisions he/she makes on its basis, deviate from the objective reality.

In this context, two points should be stressed. First of all, if there is an oversupply of information and *attention crash*, it is necessary to create an information filter, so that the recipient can receive only that information that he/she considers necessary, interesting, or corresponding to his/her beliefs. This allows the recipient to avoid information he/she believes is not needed, not interesting, or contradicting his/her beliefs and judgements, which in turn allows for (often subconscious) avoidance of cognitive dissonance. This is particularly important in a situation when information contradicts the model of reality created by the recipient. This creates an *information bubble* – the recipient pays attention only to the information that is consistent with the model he/she created and omits the rest. The recipient searches for and accepts only the information that confirms his/her previous ideas and beliefs. In the process of perceiving reality there is a natural tendency to "match" facts with previously accepted assumptions or theories. In extreme cases, "not matching" facts are simply ignored and/

[9] See: A. Kępiński, *Lęk*, Kraków 2007, p. 20 *et seq.*; *idem*, *Melancholia*, Warszawa 1974, pp. VI–VII, 156–254.

or treated as "invalid", "not affecting" the overall assessment. The mechanism of cognitive dissonance mentioned above consists, in a nutshell, in ignoring or even rejecting facts that "do not match" the image of reality created by the viewer, thus excluding the recognition of all issues that do not support the validity of the assumptions made earlier. On the other hand, the significance of facts confirming their validity is then overestimated, and sometimes – in extreme cases – the viewer may even see non-existent facts. In other words, analysts then see only what they want to see, as this fits within the framework of their assumptions. It is obvious that such an attitude also affects how the viewer assesses the credibility of and confidence in information sources – sources of facts "matching" the concept are treated as reliable and vice versa.[10] Needless to say, decisions made on this basis do not correspond to reality.

Second of all, this creates a field for information manipulation. After identifying the recipient's information preferences, it is possible to create the scope of his/her information bubble, drawing his/her attention to specific information that fits within this bubble and may shape the model of reality created by the recipient. In this way, it is possible to create a situation in which the recipient ignores certain facts or opinions, exaggerating others, and – in extreme cases – believing in *fake news*.

Such a situation is facilitated by the fact that an increasing number of people do not trust institutional media, believing in information coming from "people like me". The place of the official, institutional media is increasingly taken by social media, which, among all other things, are an excellent platform for the manipulation of information. Its reach, as mentioned above, is almost unlimited. Particular branches of society are therefore beginning to operate in information bubbles, choosing only the sources of information which match their beliefs and *de facto* reinforce them. The resulting space is unprecedentedly vulnerable to social manipulation, including by foreign agents.[11] This is due to the fact that an increasing number of people are using social media as a source of information; according to Pew Research Center, 44% of Americans used social media to obtain

[10] See T. Aleksandrowicz, *Podstawy walki informacyjnej*, Warszawa 2016, p. 96. For more information on the impact of cognitive dissonance on decision making, see E. Aronson, *Człowiek – istota społeczna*, Warszawa 1987, pp. 130–192, in particular 143–154.

[11] See also T. Aleksandrowicz, *Podstawy walki informacyjnej*, *op. cit.*, p. 35, 83 *et seq.*

information about the presidential campaign in 2016; other researchers report even 62%.[12] The effectiveness of these activities was undoubtedly facilitated by the above mentioned loss of trust in governments and state institutions, as well as institutional mass media, considered to present the views of the establishment, which are thus unworthy of trust. As a result, trust in "people like us", who have accounts on Facebook or Tweeter, is growing, even though some of the accounts most involved in political or emotive social issues, may beserved by Russian *information warriors*. A 2014 study by Pew Research Center shows that trust in the traditional mass media, including TV, the press, radio, or news agencies, oscillates at 50%.[13]

To summarise, one can recall a quotation by a Polish writer Jacek Dukaj: "it is not reality itself but social reactions to this reality that constitute the system of reference – and these are two completely different things".[14] When one puts it in terms of information metabolism, one can state that the model of reality created by the recipient is far from the actual reality, and therefore the decisions made on its basis are inaccurate. The recipient, in the second phase of the process, analyses his/her reality through the prism of these decisions – and thus closes the feedback loop.

The above statements justify the thesis that the key issue that determines the effectiveness of information operations is to identify the model of reality created by the recipient (the purpose of an information attack), the recipient's information preferences, and the range (shape) of his/her information bubble; and – on the basis of this knowledge – to make such a selection of skilfully crafted information that will encourage the recipient to make decisions consistent with the intention of the attacker. It should be stressed that the above refers to crafted (manipulated) information, and not simple lies, because these can be quickly verified, giving only a short-term effect. The initial information must contain some element of truth, but the truth is not emphasised as a starting point, it is placed in the context desired by

[12] See K. Pałka-Suchojad, *Wojna na tweety, czyli o weaponizacji mediów społecznościowych*, [in:] *Słowa jak kamienie. Mowa nienawiści, kłamstwo, agresja w sieci. Kompendium wiedzy o języku w życiu publicznym*, A. Kasińska-Metryka, R. Dudała, T. Gajewski (eds), Kraków – Nowy Targ 2019, pp. 102–103.

[13] National Intelligence Council, *Global Trends: Paradox of Progress*, January 2017, NIC 2017-001, https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf (accessed: 30.01.2017), pp. 199–200.

[14] J. Dukaj, *Aguerre w świcie*, [in:] *Król Bólu*, Kraków 2010, p. 712, translation: publisher.

the attacker, exaggerating some elements, or treating assumptions as facts. An example of such actions may be the Russian information campaign in 2016 aimed at weakening the position of Chancellor Angela Merkel's government. The starting point for actions aimed at detecting Russian disinformation is the observation that the method most frequently used by Russian propaganda is to inform about incidents without giving any evidence. After the assaults on women on New Year's Eve in Cologne, the Russian media blamed American CIA for the incidents. Commentators compared the events in Cologne with the pogrom of Jews in November 1938, carried out by the German Nazis. The Russian media also reported that German authorities were directing Czech prostitutes to refugee centres in order to spread venereal diseases among Czechs, as a form of punishment for Prague's refusal to accept refugees.[15]

A similar information is the alleged disappearance of a 13-year-old Russian girl living in Berlin in January 2016. The child was allegedly abducted and raped by two men from the Middle East. Even Russia's Foreign Minister Sergey Lavrov commented on the incident, expressing his hope that the migrant issues in Germany would not lead to the incident being covered up for political reasons. The Russian media reported on the incident in a very emotional fashion, and the Russian diaspora in Germany organised a march of protest. Eventually, it was discovered that 13-year-old Lisa had simply spent the night at her friend's house – she had neither been abducted nor raped.[16]

The effectiveness of such disinformation is that the society is ready to accept such crafted information and believe in it. In this case, it was reinforced by real problems that had occurred in German society after the mass influx of immigrants from the Middle East, as a consequence of Chancellor Angela Merkel's "open door" policy. In other words, information provided

[15] PAP, *Rosja chce zdestabilizować Niemcy? Rząd Merkel sprawdza*, "Interia Fakty", 19 February 2016, http://fakty.interia.pl/news-rosja-chce-zdestabilizowac-niemcy-rzad-merkel-sprawdza,nId,2147690 (accessed: 19.02.2017). Cf. //gak /, *"Nasza Liza", CIA i czeskie prostytutki. Niemcy sprawdzą, czy to rosyjski plan*, "TVN24.pl", 19 February 2016, http://www.tvn24.pl/wiadomosci-ze-swiata,2/niemiecki-wywiad-sprawdzi-dezinformacje-rosji,620678.html (accessed: 19.02.2017).

[16] *Uprowadzenie i gwałt 13-latki? Ławrow żąda od Niemiec wyjaśnień*, "TVN24.pl", 26 January 2016, http://www.tvn24.pl/wiadomosci-ze-swiata,2/rosja-siergiej-lawrow-atakuje-niemcy-pyta-o-gwalt-na-13-latce,613989.html (accessed: 19.02.2017).

by the Russian media found fertile ground in the society who was willing to believe it. Many German citizens, and some of the opposition at the turn of 2015/2016, even accused the Chancellor-in-office of making it impossible to maintain control over refugees, public order, etc.[17]

Another example is the casus from the U.S. presidential campaign in 2016, when social media were flooded with information that Hillary Clinton and John Podesta (the head of her campaign) run a secret brothel for paedophiles in Ping Pong pizzeria in Washington, D.C. One U.S. citizen, Edgar Maddison Welch, believed the news and committed an armed robbery of the premises; after being captured by the police, he testified that the information had upset him and he wanted to close the alleged brothel by force.[18]

The shape of the reality model is determined by so-called *microtargeting*, or reference to a specific recipient. Of course, in the practice of information operations, this influence is directed not at individual recipients but at groups of recipients characterised by specific features. A new branch of business has already been established – *data mining*; the companies operating in this branch are engaged in acquiring information about individuals by aggregating data from various databases, some of which are legally accessible, while access to others requires breaching the law.[19] This problem becomes politically significant if the acquired data allows to build a voter preference profile – determining a given voter's political preferences, the strength and depth of his/her beliefs, his/her openness to arguments, that is, all information making it easy to determine who he/she wants to vote for, how determined his/her beliefs are, and what arguments can change his/her decision. This entails manipulating political views and gaining influence over citizens' electoral decisions. These are not theoretical situations, because such events took place during the presidential elections in the United States in 2016, or during the referendum campaign on Brexit in

[17] See T. Aleksandrowicz, *Podstawy walki informacyjnej*, *op. cit.*, pp. 93–94.

[18] A. Abrams, *Pizzagate Gunman: 'I Regret How I Handled' Comet Ping Pong Shooting*, "Time", 8 December, 2016. https://time.com/4594988/pizzagate-gunman-comet-ping-pong-regret/ (accessed: 19.06.2020). For a detailed description of the cited examples, see: T. Aleksandrowicz, *Bieżące zagrożenia terrorystyczne. Część I. Doświadczenia ostatniego dziesięciolecia*, „Przegląd Policyjny", 2017, no. 4(128), pp. 43–45.

[19] See T. Aleksandrowicz, *Podstawy walki informacyjnej*, *op. cit.*, pp. 42–44.

Great Britain.[20] The main role in this procedure was played by Cambridge Analytica, a company that obtained data of over 87 million Facebook users. These data concerned not only users' behaviour on Facebook, but also all data made available by them while using such applications as *Mafia Wars*, *Words with Friends*, or *Farmville* – these applications had access to virtually all personal data of their users. Presenting the profiling principles developed by the company, its president, Alexander Nix, stated that psychographic profiling, on the basis of which it is possible to address the message precisely to a particular voter, is based on the OCEAN model. It establishes five personality traits, i.e. *openness* – how willingly the researched person accepts new experiences, *conscientiousness* – to what extent the person likes either order and repetitiveness or change and liquidity, *extroversion* – how sociable the person is, *agreeableness* – how willing the person is to put the needs of others above his/her own, and *neuroticism* – whether he/she is very anxious. "If you know the personality of the people you are targeting, you can nuance your messaging to resonate more effectively with those key audience groups", Nix said.[21] Vaidhyanathan refers to a report by the then Director of Facebook Security, Alex Stamos, according to which in the period from June 2015 to May 2017 about a hundred thousand dollars spent on Facebook ads, which translated into about three thousand ads, came from about 470 fake accounts and sites. These accounts were interconnected and were most likely controlled from Russia. Most of the advertisements did not directly mention the candidate's name, but clearly focused on the message deepening social and political divisions in different areas of the ideological spectrum – they raised issues of LGBT rights, racial issues, immigration, access to firearms. According to advertising specialists, these messages reached twenty three million up to seventy million people (the precise number cannot be calculated).[22]

[20] See for example S. Vaidhyanathan, *Antisocial media. Jak Facebook oddala nas od siebie i zagraża demokracji*, Warszawa 2019, p. 235 *et seq.*; A. Kazimierska, W. Brzeziński, *Strefy cyberwojny*, Warszawa 2018, p. 85 *et seq.*

[21] S. Vaidhyanathan, *Antisocial media…*, *op. cit.*, pp. 240–243, 248, 255.

[22] *Ibidem*, p. 282.

This phenomenon was observed during the presidential campaign in the United States in 2016 and, for example, during the referendum campaign on Brexit in the United Kingdom.[23]

Mechanism of information metabolism and the concept of reflexive control

The mechanism of information metabolism has found its application in Russian concepts of information operations, primarily in so-called *reflexive control*, which is used to influence the opponent's society by means of manipulation and disinformation.[24] The author of the concept of reflexive control is Vladimir Lefebvre, a Russian psychologist and mathematician living in the United States since the 1970s. The concept was developed in the 1960s, and it is currently being developed for the purposes of Russian theory and practice of information warfare. The essence of Lefebvre's concept of reflexive control is the assumption that each subject creates not only his/her own image of the material world in its consciousness, but he/she also has the ability to analyse his/her own thoughts and perceptions (self-reflection or first degree reflection).[25] With the help of appropriate instruments (e.g. provocation, intrigue, camouflage, etc.), it is possible to influence these processes from the outside. This can be done, for example, by means of transferring false information about a given situation or a false image of a given subject, or by formulating a doctrine that is beneficial for one's own interests and passing it on to one's opponent in such a way that encourages him/her to undertake actions beneficial for one. Alternatively,

[23] See for example T. Snyder, *Droga do niewolności. Rosja. Europa, Ameryka*, Kraków 2019, p. 10; S. Vaidhyanathan, *Antisocial media…*, *op. cit.*, p. 235 *et seq.*; U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election. Volume I of II. Special Counsel Robert S. Mueller, III. Submitted Pursuant to 28 C.F.R. § 600.8(c)*, Washington, D.C. March 2019 https://www.justice.gov/storage/report.pdf (accessed: 4.01.2019). Cf.: M. Wojnowski, *Wybory prezydenckie jako narzędzie destabilizacji państw w teorii i praktyce rosyjskich operacji informacyjno-psychologicznych w XX i XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego", 2019, no. 21, p. 13 *et seq.*

[24] For a more detailed discussion of the topic, see T. Aleksandrowicz, *Podstawy walki informacyjnej*, *op. cit.*, p. 161 *et seq.*

[25] A reader interested in this topic will find more information in: M. Wojnowski, *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych*, „Przegląd Bezpieczeństwa Wewnętrznego", 2015, no. 12(7), pp. 11–36.

this can also be done by means of neutralising the opponent's deductions, leading to his/her disorientation by creating a few fictitious goals that make it impossible to discover the real goal. This is how one can achieve a profound transformation of the mass consciousness of the society and change the moral and psychological state of the society.

This concept is related to the concept of *rebel war* created by Evgeny Messner. Messner's concept is based on stimulating the formation of anti-government, revolutionary groups in the opposite state that tend not to retreat from violence and take partisan or terrorist actions. The aim of a rebel war is not only to neutralise the opponent's armed forces, but also to destabilise the state by means of psychological factors (demoralisation, fear, insecurity). This is why Messner himself described rebel war as a "semi-war" – armed violence that is not classic warfare. The main goal of a rebel war is to "conquer the soul of an enemy nation", hence an important role is played by journalists, saboteurs, provocateurs, propagandists, and the notion of a front line in such a war refers to particular spheres of a given society's activity (politics, economy, culture, etc.).[26]

Among detailed rules of conducting a rebel war, Messner listed decomposition of the unity of an enemy nation, breaking its active parts (armed forces, social movements), defending the unity of one's own nation, and limiting the influence of factors that may cause a negative reaction in neutral states, not only in governmental spheres, but also in broad social groups.[27]

Practical application of these concepts can be observed by analysing the course of the Russian-Ukrainian conflict. Incidentally, it can be stated that from the perspective of the Russian Federation, Ukraine is a sort of testing ground for new solutions to the conflict in the 21st century security environment.[28]

---

[26] See M. Wojnowski, *Terroryzm w służbie geopolityki. Konflikt rosyjsko-ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji wojny buntowniczej Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego", 2015, no. 11(6), pp. 73–77; J. Tomasiewicz, *Od skrytobójstwa do miatieżowojny. Ewolucja terroryzmu politycznego w Europie – aspekty ideologiczne, taktyczne i organizacyjne*, „Przegląd Bezpieczeństwa Wewnętrznego", 2014, no. 11(6), pp. 133–134.

[27] M. Wojnowski, *Terroryzm w służbie geopolityki…*, *op. cit.*, pp. 76–77.

[28] See B. Pacek, *Wojna hybrydowa na Ukrainie*, Warszawa 2018; B. Pacek, P. Pacek, *Psychologia wojny hybrydowej*, Warszawa 2019; T. Aleksandrowicz, *Wywiad jako narzędzie w koncepcji nowych wojen*, „Studia Politologiczne", 2017, no. 43, p. 165 *et seq.*;

Conclusions

The considerations presented above allow for several conclusions. First, the concept of information metabolism is applied in relation to contemporary information operations aimed at influencing the behaviour of societies, also in the political dimension. The assessment of such information in terms of using information metabolism explains the mechanism of its effectiveness.

Second, the basic condition for the effectiveness of an information operation is to identify information preferences of the target and the model of reality created by the target, and then to craft the transferred information in such a way that it fits into the target's information bubble and reaches him/her through information channels that he/she considers credible. Social media play a special role in this respect, treated – in view of the decline of the public's confidence in the institutional media linked to the establishment – as the "voice of people like me".

Third, the starting point (axis) in preparing an act of manipulation is information about a fact or event that is embedded in the information reality perceived by the target. This fact is presented in an exaggerated context, convenient for the attacker.

Fourth, combating this type of information attacks and their consequences is an extremely difficult task and requires the state to achieve both defensive and offensive capabilities in the area of information warfare. The mere recognition of an attack and denying *fake news* are not a sufficient solution, because if it turns out that a given piece of information was false and the state manages to prove it to those who believed the disinformation, all the senders lose their credibility, because the recipient can state: "What is the truth? Everyone is lying!". This way the circle closes, and distrust may be the intended target of the attacker.

Achieving such capabilities by the state means, above all:

- the ability to recognise the intentions and goals of a potential attacker;
- recognising potential information threats;
- the ability to identify one's own weaknesses (weak points), which may become the axis of an information attack;

T. Aleksandrowicz, A. Bógdał-Brzezińska, J. Gryz, I. Oleszkiewicz, G. Ostasz, *Walka informacyjna w społeczeństwie sieciowym. Uwagi na tle kryzysu ukraińskiego*, [in:] *Terroryzm i cyberterroryzm jako największe wyzwanie dla bezpieczeństwa współczesnego państwa*, Chicago 2016, p. 119 *et seq.*

- preparing one's own narrative/response to an information attack;
- having and being able to use information channels that are reliable for one's citizens.

Of course, it is also necessary to educate the public, to develop research in the presented area, and to use the practical results of this research. It is therefore necessary for governmental circles to cooperate with scientific and academic centres, think tanks, and representatives of the broadly understood civil society.

References

Literature:

1. Aleksandrowicz T., *Bezpieczeństwo informacyjne państwa*, „Studia Politologiczne", 2018, no. 49.
2. Aleksandrowicz T., *Bieżące zagrożenia terrorystyczne. Część I. Doświadczenia ostatniego dziesięciolecia*, „Przegląd Policyjny", 2017, no. 4(128), pp. 27–47.
3. Aleksandrowicz T., *Infosfera jako środowisko bezpieczeństwa państwa. Próba konceptualizacji problemu*, [in:] *Nauka i praktyka bezpieczeństwa. Księga pamiątkowa Leszka Fryderyka Korzeniowskiego, profesora Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie*, A. Kozera, E. Sadowska (eds), Kraków 2019.
4. Aleksandrowicz T., *Podstawy walki informacyjnej*, Warszawa 2016.
5. Aleksandrowicz T., *Świat w sieci. Państwa. Społeczeństwa. Ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, 2nd edition, Warszawa 2018.
6. Aleksandrowicz T., *Wojna jako narzędzie polityki w XXI wieku. Stare pojęcia – nowe konotacje*, [in:] *Siła we współczesnych stosunkach międzynarodowych*, W. Kostecki, K. Smogorzewski (eds), Warszawa 2017.
7. Aleksandrowicz T., *Wywiad jako narzędzie w koncepcji nowych wojen*, „Studia Politologiczne", 2017, no. 43, pp. 165–193.
8. Aleksandrowicz T., Bógdał-Brzezińska A., Gryz J., Oleszkiewicz I., Ostasz G., *Walka informacyjna w społeczeństwie sieciowym. Uwagi na tle kryzysu ukraińskiego*, [in:] *Terroryzm i cyberterroryzm jako największe wyzwanie dla bezpieczeństwa współczesnego państwa*, Chicago 2016, pp. 119–158.
9. Aronson E., *Człowiek – istota społeczna*, Warszawa 1987.

10. Dukaj J., *Aguerre w świcie*, [in:] *Król Bólu*, Kraków 2010.
11. Eco U., *Temat na pierwszą stronę*, Warszawa 2015.
12. Gleick J., *The Information. A Theory. A History. A Flood*, New York 2011.
13. Kazimierska A., Brzeziński W., *Strefy cyberwojny*, Warszawa 2018.
14. Kisilowska M., *Przestrzeń informacyjna jako termin informatologiczny*, „Zagadnienia Informacji Naukowej", 2011, no. 2, pp. 35–52.
15. Kępiński A., *Lęk*, Kraków 2007.
16. Kępiński A., *Melancholia*, Warszawa 1974.
17. Madej M., *Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego*, [in:] *Bezpieczeństwo teleinformatyczne państwa*, Madej M., Terlikowski M. (eds), Warszawa 2009, pp. 17–40.
18. Pacek B., *Wojna hybrydowa na Ukrainie*, Warszawa 2018.
19. Pacek B., Pacek P., *Psychologia wojny hybrydowej*, Warszawa 2019.
20. Pałka-Suchojad K., *Wojna na tweety, czyli o weaponizacji mediów społecznościowych*, [in:] *Słowa jak kamienie. Mowa nienawiści, kłamstwo, agresja w sieci. Kompendium wiedzy o języku w życiu publicznym*, A. Kasińska-Metryka, R. Dudała, T. Gajewski (eds), Kraków – Nowy Targ 2019.
21. Snyder T., *Droga do niewolności. Rosja. Europa, Ameryka*, Kraków 2019.
22. Sosińska-Kalata B., *Obszary badań współczesnej informatologii (nauki o informacji)*, "Zagadnienia Informacji Naukowej", 2013, no. 51, pp. 9–41.
23. Tomasiewicz J., *Od skrytobójstwa do miatieżowojny. Ewolucja terroryzmu politycznego w Europie – aspekty ideologiczne, taktyczne i organizacyjne*, „Przegląd Bezpieczeństwa Wewnętrznego", 2014, no. 11(6), pp. 115–136.
24. Vaidhyanathan S., *Antisocial media. Jak Facebook oddala nas od siebie i zagraża demokracji*, Warszawa 2019.
25. Wojnowski M., *Terroryzm w służbie geopolityki. Konflikt rosyjsko-ukraiński jako przykład realizacji doktryny geopolitycznej Aleksandra Dugina i koncepcji wojny buntowniczej Jewgienija Messnera*, „Przegląd Bezpieczeństwa Wewnętrznego", 2015, no. 11(6), pp. 73–77.
26. Wojnowski M., *Wybory prezydenckie jako narzędzie destabilizacji państw w teorii i praktyce rosyjskich operacji informacyjno-psychologicznych w XX i XXI wieku*, „Przegląd Bezpieczeństwa Wewnętrznego", 2019, no. 21.
27. Wojnowski M., *Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych*, „Przegląd Bezpieczeństwa Wewnętrznego", 2015, no. 12(7), pp. 11–36.

Documents:
1. National Intelligence Council, *Global Trends: Paradox of Progress*, January 2017, NIC 2017-001, https://www.dni.gov/files/documents/nic/GT-Full-Report.pdf (accessed: 30.01.2017).
2. U.S. Department of Justice, *Report on the Investigation into Russian Interference in the 2016 Presidential Election. Volume I of II. Special Counsel Robert S. Mueller, III. Submitted Pursuant to 28 C.F.R. § 600.8(c)*, Washington, D.C. March 2019 https://www.justice.gov/storage/report.pdf (accessed: 4.01.2019).

Mass media:
1. //gak /, *"Nasza Liza", CIA i czeskie prostytutki. Niemcy sprawdzą, czy to rosyjski plan*, "TVN24.pl", 19 February 2016, http://www.tvn24.pl/wiadomosci-ze-swiata,2/niemiecki-wywiad-sprawdzi-dezinformacje-rosji,620678.html (accessed: 19.02.2017).
2. Abrams, A., *Pizzagate Gunman: 'I Regret How I Handled' Comet Ping Pong Shooting*, "Time", 8 December, 2016. https://time.com/4594988/pizzagate-gunman-comet-ping-pong-regret/ (accessed: 19.06.2020).
3. PAP, *Rosja chce zdestabilizować Niemcy? Rząd Merkel sprawdza*, "Interia Fakty", 19 February 2016, http://fakty.interia.pl/news-rosja-chce-zdestabilizowac-niemcy-rzad-merkel-sprawdza,nId,2147690 (accessed: 19.02.2017).
4. *Uprowadzenie i gwałt 13-latki? Ławrow żąda od Niemiec wyjaśnień*, "TVN24.pl", 26 January 2016, http://www.tvn24.pl/wiadomosci-ze-swiata,2/rosja-siergiej-lawrow-atakuje-niemcy-pyta-o-gwalt-na-13-latce,613989.html (accessed: 19.02.2017).

Cite this article as:
T. Aleksandrowicz, *The concept of information metabolism by Antoni Kępiński and the mechanism of information manipulation. Conditions for effectiveness and ways of counteraction*, "Security Dimensions", 2020, no. 33, pp. 150–165, DOI 10.5604/01.3001.0014.2675.