WIEDZA OBRONNA
2022, Vol. 280 No. 3
ISSN: 2658-0829 (Online) 0209-0031 (Print)
Journal homepage: http://wiedzaobronna.edu.pl
DOI: https://doi.org/10.34752/2022-c280

WIESŁAWA ZAŁOGA*
Wojskowa Akademia Techniczna, Warszawa, Polska

DISINFORMATION IN THE AGE OF THE DIGITAL REVOLUTION IN THE ASPECT OF STATE SECURITY

ABSTRACT: The main purpose of the article is to diagnose the awareness and attitudes of respondents towards the fake news and disinformation on the Internet. The following hypothesis was set within the framework of the presented objective: the phenomenon of disinformation contributes to the creation of a sense of threat and arousal of social unrest. Two research approaches were used in the research process - the first was based on quantitative study using a questionnaire as a method of data collection, and the second was relied on general content analysis of the literature on the subject and netographic content. The findings of the research allowed to determine the priority measures for taking action against disinformation. The assumptions of the article correspond to the current challenges in the issue of fighting disinformation and thus establishing strategies to counter disinformation. The main research limitations were the restricted sample size, limited generalizability in the conducted analysis of the content of the literature, and the broad scope of the study resulting from the areas of knowledge, skills and attitudes regarding awareness of disinformation presence on the Internet.

KEYWORDS: disinformation, digital revolution, security, threat.

INTRODUCTION

In the era of the digital revolution, the vast majority of threats to community security are related to information security, resulting in a major transformation of national security systems that affect state security. Internet services have provided societies around the world with new ways and quality of communicating and obtaining and transmitting information. However, the

* **dr Wiesława Załoga**, , Military University of Technology, Warsaw, Poland
https://orcid.org/0000-0001-7758-0187, wieslawa.zaloga@wat.edu.pl

dissemination of messages that intentionally mislead the recipient is becoming a huge problem and a threat to the proper functioning of a democracy. The present times are often referred to in scientific publications as the era of fake news, disinformation or the era of information chaos. In the mass media we come across a huge amount of incomplete information, which misleads the viewer and brings about information chaos. This state of information chaos is designed to influence the behavior of the recipient and result in destabilization. Nowadays, the received information in the modern public space can be deformed and thus distorted, which is referred to in the literature as disinformation.

Disinformation these days has taken various forms, such as hostile propaganda, ideological diversion, trolling or malicious moderation of discussions on forums[1] and on social media. By adopting an appropriate strategy, it often uses means that are tailored to the specifics of countries, societies and particular target groups to distort the truth, spread distrust or create doubt[2]**.** Disinformation is the deliberate creation and dissemination of false and or manipulated information intended to deceive and mislead recipients, whether to cause harm, or for political, personal or financial gain[3].

Disinformation is assessed as a threat that can be used deliberately to gain an advantage, e.g. military or economic. Disinformation in the general sense refers to false information disseminated with the purpose of deliberately misleading or deceiving people. It refers to the dissemination of false information, regardless of whether its purpose is to deceive or mislead a person. Disinformation is most often used on a large scale. It can refer, for example, to a disinformation campaign by a country's government aimed at the society of another country. Disinformation, in the example cited, can mean the dissemination of false information regarding a country's military strength and plans, spread by the government or intelligence agencies in tactical political diversion activities. It can threaten public security, community cohesion, can reduce trust in government institutions and the media, undermine the integrity of a country's government and democratic processes, harm a country's economic well-being locally and globally. Disinformation is delivered to intentionally mislead a selected audience and induce them to follow the assumptions expected by the sender. The most dangerous and

[1] Y. Benkler, R. Faris, H. Roberts, „N*etwork Propaganda: Manipulation, Disinformation, and Radicalization in American Politic*s", OXFORD University Press, New York USA, 2018, p. 12-13.
[2] M. Wrzosek, *„Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*", NASK Cyber POLICY, NASK Państwowy Instytut Badawczy, Warszawa 2019, p. 9.
[3] A. Aiken, *„RESIST Counter-disinformation toolkit"*, p. 6, (accessed: 22.07.2022).

powerful aspect of disinformation is quite often the perceived grain of truth, which undoubtedly makes disinformation much more credible. Undoubtedly, nowadays disinformation is a powerful weapon, devastating and dividing societies. It is also a common tool of the intelligence community. Increasing disinformation is most often seen among rival circles such as the Russian Federation and Ukraine or the European Union. Disinformation relating to the cited countries is coordinated on a large scale as an elaborate plan to spread misinformation, and we can undoubtedly call it a disinformation campaign on a global scale.

Disinformation is a phenomenon considered nowadays to be one of the most serious challenges of today's Internet, and it takes place with very high intensity. Introducing disinformation into the social environment of another country can lead to the destabilization of society and the state. Disinformation during a military crisis in a particular region is especially dangerous from a global perspective. In its disinformation campaign strategy, the Russian Federation is attempting to influence the relations of allied states as well as to cause a split between allies, and to undermine the credibility of international institutions. In this instance, the disinformation narrative in the Russian Federation media is trying to prove that NATO, for example, is an unreliable and unnecessary organization. In the case of Poland, the Russian Federation's disinformation narrative resounds in the field of undermining the credibility of Polish uniformed services, armed forces, government offices, professional circles, etc. The Russian Federation, creating a policy of disinformation, is undoubtedly making efforts to influence Polish politics in the international environment and Poland's relations with other countries, i.e. it is unquestionably aimed at worsening political and diplomatic relations.

Disinformation has significantly gained momentum with the development of the Internet and social networks. It is the Internet that has made it possible to influence or manipulate public opinion on an unprecedented scale. This publication analyzes the impact of disinformation in the age of digital society on state security in terms of the threats posed by the pursuit of aggressive policies of a country against another country using the opinions of respondents obtained through surveys. Accordingly, the study explores some of the processes evident at the international level and reviews some external national security issues. The research methods and techniques implemented in the research process itself are based primarily on a critical analysis of the literature and an analysis and synthesis of published research outcomes as well as an analysis of the results of a survey of 164 respondents of managers of small, medium and large companies in 16 provinces in Poland from May 16-20, 2022. The author's survey was designed to investigate respondents' awareness and attitudes toward the existence of fake news and misinformation on the Internet. The survey addressed the following specific issues:

- The level of trust in news and information provided through various information channels;
- Respondents' perceptions of how often they encounter news or information that is misleading or fake;
- respondents' confidence in identifying news or information that is misleading or fake;
- respondents' view of the scale of the disinformation problem in cyberspace;
- the view of what institutions and media actors should do to stop the spread of fake news.

The findings show that the phenomenon of disinformation, which intensifies in crisis situations, such as those related to the outbreak of war in Ukraine or a pandemic, contributes to the destabilization of public sentiment, impedes the functioning of the basic organs of the state, and consequently increases the negative effects of crisis events. In addition, the disinformation used during the military actions of the Russian Federation in Ukraine has intensified its effects, causing damage on a huge scale. The analysis shows that the fight against disinformation must be based on the assumption that state security depends primarily on the information awareness of every citizen of a country. Public awareness is built through effective education aimed at raising basic knowledge of a country's strength and credibility and economic and military stability. Disinformation in the digital age has tremendous power of influence and raises serious consequences for countries, as it poses a new threat to their national security in peacetime. The development of the information society, coupled with the expansion of the reach of the Internet, is accompanied by the penetration of aspects of human activity into cyberspace. The worldwide reach and the possibility of instant access from almost anywhere on Earth, combined with the low cost of use, has led more and more entities, as well as individuals, to move their daily activities into cyberspace. Many Internet users cannot imagine life without quick access to information and e-mail, online banking, online shopping, electronic ticket reservations or contact with family and friends through social networks and instant messaging. Accessible via computers, cell phones, tablets and even cars, the Internet has become one of the primary utilities, along with electricity, gas and running water. It has grown to become synonymous with freedom of speech and the unfettered flow of information, and in many cases has successfully served as a tool for revolution or social change.

THE ROLE OF THE STATE IN FIGHTING DISINFORMATION AS A THREAT

In order to understand propaganda activities and identify methods and ways to counter disinformation, it is necessary to define the basic concepts of information combat in cyberspace such as information warfare, strategic communication, information operations, psychological operations and disinformation.

Information warfare, which can most briefly be defined as the use of a variety of means to gain information advantage[4], is a term that is constantly being redefined, and defense experts are still arguing over the basic concepts associated with it. However, there is a consensus that information itself has become a strategic resource used on many battle fronts. Information warfare is not only a matter of using information and information technology to defeat the enemy on the battlefield, but also of protecting one's own systems and information, critical to the proper functioning of society.

Strategic communications, to paraphrase the 2009 *NATO Strategic Communications Policy* definition, is the coordinated and appropriate use of communications activities and capabilities (public diplomacy, press and information activities, information operations, psychological operations) in support of policy, operations and activities[5]. It involves communicating (conveying) meaning to support the goals set. It involves listening as much as it does broadcasting[6]. According to the definition of the National Security Bureau, strategic communication is a synthesis of information activities (public diplomacy, public communication, information operations, psychological operations) of a given strategic entity aimed at shaping the views and decisions of other entities in the strategic environment in a way that is beneficial to its own strategic interests[7]. In the civilian scientific community, strategic

[4] K. Rokiciński, B. Pac, *„Operacje informacyjne w działaniach militarnych"*, Wydawnictwo J.P., Gdynia 2010, p. 21.

[5] *NATO Strategic Communications Policy*, https://publicintelligence.net/nato-stratcom-policy (accessed: 12.04.2022).

[6] *Strategic Communication Joint Integrating Concept,* http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jic_strategiccommunications.pdf?ver=2017-12-28-162005-353 (accessed: 11.04.2022).

[7] *(MINI) Słownik BBN - Propozycje nowych terminów,* https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (accessed 11.05.2022).

communication is most often understood as a field that combines theories, models and methods from several scientific fields such as marketing, public relations, corporate communication, business communication and organizational behavior[8].

Information operations as defined by the 2018 DOD *Dictionary of Military and Associated Terms* include the integrated use of information capabilities in conjunction with other lines of action to shape, disrupt, corrupt, or take over decision-making processes (influencing the will, understanding, capabilities[9]) of opponents and potential adversaries while protecting its own decision-making processes [10]. Similarly, the term information operations was defined by the National Security Bureau [11] broken down into: offensive operations: psychological operations, simulation, destruction, electronic warfare, information attacks, social communication operations; defensive operations: information security, cover, counter-propaganda operations, counter-intelligence operations, electronic combat, information special operations[12].

Psychological operations according to *NATO Strategic Communications Policy* are planned psychological activities carried out through communication methods and other means aimed at approved audiences in order to influence their perceptions, attitudes and behavior for the achievement of political and military objectives[13]. According to the non-military definition of the National Security Bureau, psychological operations are those aimed at affecting the emotions, motivations, objective reasoning of foreign governments, organizations, groups and individuals who are the audience of these operations, so as to achieve the effect of behavior favorable to the pursuit of their own interests[14].

Psychological operations (activities) play a dominant role in information (offensive) operations, so that the two terms are often confused and used interchangeably as synonyms. It is possible that such a "swap" of terminology is intentional, since psychological operations, which can also include propaganda, are rightly viewed negatively by the public and groups interested in their use (e.g., politicians) prefer to use the neutral but erroneous term

[8] Wilbur D., *„Propaganda's Place in Strategic Communication: theCase of ISIL's Dabiq", Magazine,* „International Journal of Strategic Communication" 2017, Vol. 11., No. 3, s. 209-223.

[9] *NATO Strategic Communications Policy*, https://publicintelligence.net/nato-stratcom-policy, (accessed: 11.05.2022).

[10] *Strategic Communication Joint Integrating Concept,* ibidem.

[11] (*MINI) Słownik BBN - Propozycje nowych terminów,* ibidem.

[12] Ibidem (accessed: 11.05.2022).

[13] *NATO Strategic Communications Policy*, https://publicintelligence.net/nato-stratcom-policy (accessed: 11.05.2022).

[14] *(MINI) Słownik BBN - Propozycje nowych terminów,* ibidem.

information operations to describe them. Psychological operations were originally called propaganda operations[15].

Propaganda, according to the definition of Henryk Kula, is a process of deliberate, persuasive political, social and ideological influence on collectivities and individuals, seeking through the formation of human attitudes to induce desired behavior[16]. This term is similarly defined by the National Security Bureau as the dissemination of manipulated and/or fabricated information in order to induce the audience to behave in certain ways favorable to the propagandist. National Security Bureau experts describe propaganda and disinformation as synonymous terms[17].

Strategic communication and its elements (information operations, psychological operations, counter-propaganda) are an important element of EU and NATO cooperation in the face of the threat from the Russian Federation and non-state actors - terrorist organizations. "The Global Strategy for the European Union's Foreign and Security Policy" of 2016 and documents as amended envisages strengthening the EU's strategic communication activities in close cooperation with NATO partners. "The Common Framework for Countering Hybrid Threats" of the same year - based on the European Security Agenda - requires coordinating strategic communication mechanisms to counter disinformation.

Disinformation activities have been carried out in various forms since ancient times, but it was only at the turn of the 20th and 21st centuries that they became a very significant security threat to both local communities and the world as a whole.

The genesis of modern disinformation is inextricably linked to globalization, the development of mass society and the intensification of media activity in public life. Technological advances in communication and information exchange have caused the media to increasingly influence public opinion. Their relentless pursuit of sensation is determined not only by the desire for profit. It also has a psychological basis, as audiences in the 21st century primarily seek "strong sensations" in the media.

This is where a profound relationship arises between media cyberspace and disinformation. Attacks in cyberspace in the form of disinformation become messages directed at the public

[15] Z. Modrzejewski, *„Operacje Informacyjne”*, AON, Warszawa 2015, p. 41-44.

[16] H. M. Kula, *„Propaganda współczesna. Istota – właściwości”*, Wydawnictwo Adam Marszałek, Toruń 2005, p. 219.

[17] *(MINI) Słownik BBN - Propozycje nowych terminów,* ibidem.

and publicized through the mass media, which use published information to attract the attention of the largest possible audience. At the same time, the larger the audience, the greater the chances of achieving the intended result by the environment that undertakes disinformation activities.

In order to cause an increase in the level of security of citizens and build their knowledge, skills and attitudes, it therefore becomes crucial to develop intensive cooperation between the media and the authorities. First of all, it is necessary to ensure that information about threats and all kinds of unfavorable social phenomena is transmitted in the right way and to the right extent. It is important to maintain good relations between the authorities and the mass media, so that both sides in a competitive environment, wanting to show their superiority, do not negatively affect public sentiment and the sense of security of citizens. In addition, attention should be focused on promoting education and prevention of potential threats in the public media[18]. Citizens feel safer when they have knowledge of how to prevent and prepare for the occurrence of possible dangers, and when they are able to respond to them and take control of them.

In the modern world, the term "security" is used more often than ever before in the history. This is because security is a widely recognized value that is placed high in the hierarchy of needs. Research on security is carried out in the social as well as the exact sciences - starting with philosophy and ending with technical sciences. The ubiquity of the use of the term causes it to be understood in a variety of ways. The simplest and, at the same time, the most widely used definition of the issue in question is the phrase defining it as "a state without threats." The above definition is derived from the original etymological meaning of the word "security" originating from the Latin language - *securitas*, composed of two members: *sine* (without) and *cura* (fear, apprehension, worry)[19].

Security is also defined as a process during which the state of security and its organization are dynamically transformed under the influence of changes in conditions. This means that security is not permanent and given once and for all.

[18] M. Kwiecińska, *„Wykorzystanie mediów dla podniesienia bezpieczeństwa, potrzeby i sposoby realizacji"*, Obronność. Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia", no 3/2014, Akademia Obrony Narodowej, Warszawa 2014, p. 81-84.

[19] J. Kaczmarek, A. Skowroński, *„Bezpieczeństwo Świat – Europa - Polska",* Wrocław, 1998*,* p. 5.

Specialists agree that security is understood as freedom from threats to fundamental values. However, a disagreement exists on the level of its guarantee, that is, whether security should be an individual, national or international issue[20].

In considering the meaning of the term "security" it is important to emphasize that it guarantees the successful development of human beings as individuals, social groups, states or international collectives. It is a concept that encompasses many aspects of social life in which any threat may occur. Among other reasons, it is treated as a universal value. In view of the above considerations, a key conclusion emerges that the absence of a threat is an essential aspect of the existence of security.

Therefore, what is a threat? In the social sciences, it is defined as potential or existing situations, phenomena or actions that pose a danger to the health and life of the population, their property and living conditions, as well as the environment, harming national interests and values, thereby contributing to the destabilization of social life and undermining the development[21].

In addition, the threat can be defined as:

- danger;
- the threat of harm, injury, or loss of health;
- risk;
- a situation or potential conditions that could result in losses as a consequence [22].

Threat is also seen as a state of consciousness created by the perception of phenomena judged to be dangerous. In this view, it is subjective in nature and depends on the assessments formulated by a particular subject[23].

However, the term "threat", which is variously understood, always means an incident judged to be dangerous or unfavorable. The reason for finding oneself in a situation in which the subject is in a state of fear and uncertainty is primarily due to an actual action taken by

[20] M. Gracik, K. Żukowska, *„Bezpieczeństwo międzynarodowe. Teoria i praktyka*,” Szkoła Główna Handlowa, Warszawa 2006, p. 21.

[21] R. Zięba, *„Pojęcie i istota bezpieczeństwa państwa w stosunkach międzynarodowych”*, „Sprawy międzynarodowe”, nr 10/1989, Polski Instytut Spraw Międzynarodowych, Warszawa 1989, p. 49-51.

[22] T. Szopa, *„Koncepcja graficznego przedstawiania terytorialnego rozkładu ryzyka i zagrożeń”*, [in:] J. Wolanin (ed.) *„Mapy terytorialnego rozkładu ryzyka”,* Wydawnictwo EDURA, Warszawa 2004, p. 22-25.

[23] Z.J. Piertaś, *„Podstawy teorii stosunków międzynarodowych”*, Uniwersytet Marii Curie-Skłodowskiej, Lublin 1986, p. 161-163.

another participant in social life, which is a real threat to the basic values and vital interests of the individual in question.

Regardless of the differences in defining and perceiving threats, knowledge of them is now becoming a basic element necessary to take preventive measures and to possibly prepare for their occurrence in order to minimize adverse effects.

The list of threats to the modern world is very long and is still expanding, so it is very difficult to list all the dangers facing the world and, above all, man. As a result of the development of globalization and the obliteration of the boundaries between the non-military and military areas, as well as the emergence of unidentified, previously unknown threats, it is necessary to create a new catalog of security threats[24].

Disinformation is an indisputable negative consequence of the process of globalization and civilization development projecting the shape and level of security, and at the same time a source of many challenges for the international community. Like the terms security and threat, disinformation is currently a popular subject of scientific studies, which does not have a uniform, universally accepted definition.

Disinformation is an evolving threat that requires continuous efforts to address the problem by engaging the right actors, tools, methods, setting priority targets and strategies. Some forms in particular of state-caused disinformation are being analyzed by the EU Hybrid Fusion Cell, in cooperation with the Strategic Communication Task Forces of the European External Action of the Services and with the support of Member State forces[25].

Disinformation can destabilize a country, have a corrosive effect on its administrative and decision-making structures, and undermine its social, economic and cultural foundations. According to the report Freedom on the Net 2077; Manipulating Social Media to Undermine Democracy[26] more and more countries around the world are using social media for disinformation activities. Both to shape their internal policies and to influence other countries. Countering disinformation is becoming a challenge addressed not only by individual states, but also by international institutions and organizations. The need to counter disinformation

[24] I. Grabowska-Lepczak, M. Kwiatkowski, M. Tryboń, *„Bezpieczeństwo człowieka w obliczu XXI wieku"*, „Zeszyty Naukowe Szkoły Głównej Służby Pożarniczej", no 41/2011, Warszawa 2011, p. 191-202.

[25] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Action Plan against Disinformation, Brusseles, 2018, p. 3.

[26] Raport, *„Freedom on the Net 2017. Manipulating Social Media to Undermine Democracy*" https://freedomhouse.org/report/freedom-net/freedom-net-2017, (accessed: 14.04.2022).

campaigns in Europe was first emphasized by the European Council in March 2015[27]. Since then, several teams have been formed within the structures of the European External Action Service to analyze disinformation in the European Union and neighboring countries of the community[28].

According to the EU's Hybrid Threat Information Synthesis Unit, it was disinformation from the Russian Federation that was expected to pose the greatest threat ahead of the May 2019 European Parliament elections[29]. Disturbing reports about the scale and impact of disinformation campaigns made 2018 a time of particularly intense work in the European Union in this regard. A total of four relevant documents were published addressing the issue of disinformation[30].

To effectively counter disinformation and build public awareness, the state' role must be leading. In the aspect of countering disinformation, the welfare of the citizen's information security must be taken care of. It is necessary to build its awareness, shape knowledge, skills and attitudes in the aspect of disinformation phenomenon. It is necessary to conduct research and raise citizen awareness of disinformation and content manipulation in a continuous process. Analysis of the literature on the subject and published studies show that when users become more aware of content manipulation and disinformation they often take actions to protect themselves and other users.

The formation of citizens' awareness should be based on institutional cooperation, which in turn necessitates the expansion of institutional capacity to counter foreign disinformation concerning a country. Another action at the state level should be the development of international cooperation. This provides an opportunity to exchange information on current and forecasted threats and on the most effective projects that support efforts to combat disinformation and, at the same time, to obtain information on emerging trends with, for

[27] Rada Europejska, Sekretariat Generalny Rady, Posiedzenie Rady Europejskiej (19 i 20 marca 2015 r.) – Konkluzje, Bruksela, p. 5.

[28] East Strategie Communication Task Force (czerwiec 2015) -for the Eastern Partnership countries; Western Balkans Task Force (December 2015) - for the Western Balkans; Task Force South (June 2017) - for the Middle East, North Africa and the Gulf region; EU Hybrid Fusion Cell - a point of analysis for hybrid threats, including disinformation campaigns.

[29] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Action Plan against Disinformation, Brusseles, 2018, p. 4

[30] Dezinformacja, www.cyberpolicy.pl (accessed: 14.05.2021).

example, technological advances. In addition, another area in which efforts to counter disinformation should be intensified is the cooperation of allied countries.

The state undertakes a variety of activities, treating the issue of disinformation holistically and using the enormous potential in the form of Polish foreign posts (embassies, consulates, Polish institutes) around the world. The actions are dictated, among other things, by the situation in the East of Poland. The policy of the Russian Federation towards Poland is unprecedentedly aggressive especially after the attack on Ukraine. This is accompanied by intensified measures in the form of information and propaganda warfare, attempts to destabilize the situation in the regions, maintaining frozen conflicts and terror attacks carried out on the territory of NATO and EU member states[31].

The Council of the European Union first recognized the threat posed by online disinformation campaigns in 2015. In 2018, EU activity in the area of countering disinformation increased significantly. The reason was the threat of disinformation and cyberattacks against the 2019 European Parliament elections, as well as against more than 50 electoral processes in member states by 2020[32].

To meet expectations, the Ministry of Foreign Affairs of the Republic of Poland focuses its activity primarily on: raising officials' awareness of disinformation threats; building the institutional capacity of the Ministry of Foreign Affairs; cooperating with strategic communication institutions in EU and NATO countries and institutions; designing and implementing active measures, i.e. conducting projects and information campaigns; cooperating with and supporting Polish NGOs[33].

Strengthening Poland's institutional capabilities, constant identification of disinformation threats, cooperation with foreign partners in NATO and the EU, among others, taking specific initiatives and training activities are tangible Polish efforts to counter and combat foreign disinformation against Poland[34].

Considering the above, preventive measures, in the form of a study tailored to the current challenges of the state security system and the international environment, remain a key issue in reducing the risk of carrying out an attack. The professional response of the services

[31] M. Wrzosek, *„Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes”*, NASK Cyber POLICY, NASK Państwowy Instytut Badawczy, Warszawa 2019, p. 11.

[32] Ibidem, s. 12.

[33] Ibidem, s. 11.

[34] Ibidem, s. 12.

responsible for international security and the security of individual states is also of great importance. After all, it is their area of responsibility to publicly announce the threat and to act efficiently to minimize losses and inhibit widespread panic or disorganization when a terrorist event occurs.

According to the EU Anti-Disinformation Action Plan of December 5, 2018: disinformation is understood "as verifiably false or misleading information that is created, presented and disseminated for economic gain, or to deliberately deceive the public, and may do public harm."

Security has very many definitions. Researchers agree that it is impossible to provide a clear definition of security. The most common one is a state (the achieved sense of security of an entity), as well as a process (providing a sense of security to an entity).[35] Security has been, is, and probably will be for a long time to come, perceived, grasped and defined very differently. The differences in the perception of security as an entity of functioning of all subjects of cognition primarily stem from the diversity of perceptions of these objects and the needs of the entity defining them[36].

Currently, there are many categories of security, among which information security has its place. As one of many researchers, Piotr Potejko defined information security as: "a set of activities, methods and procedures undertaken by authorized entities aimed at ensuring the integrity of collected, stored and processed information resources, by securing them from unwanted, unauthorized disclosure, modification or destruction"[37].

Another definition of information security is the protection of information from unwanted (accidental or deliberate) disclosure, modification, destruction, or preventing its processing. The progress of civilization, the development of the media, the expanding stock of information shape new phenomena, expanding the catalog of national security to new areas, as was the case with information security.

PUBLIC AWARENESS IN THE ASPECT OF DISINFORMATION IN CYBERSPACE

It is undeniable that the Internet has opened up enormous opportunities for the development of social activity in the realms of politics, democracy and security. In order to use

[35] S. Koziej, ,,*Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*", Warszawa 2011, (accessed: 21.05.2022).

[36] B. Zdrodowski, „*Istota bezpieczeństwa państwa*", Wyższa Szkoła Policji w Szczytnie, (accessed: 21.05.2022).

[37] P. Potejko, „*Bezpieczeństwo informacyjne*", [in:] „*Bezpieczeństwo państwa*", K.A. Wojtaszczyk, A. Materska-Sosnowska (eds.), Oficyna Wydawnicza ASPRA-JR, Warszawa 2009, p. 193.

the technology as effectively and consciously as possible, each individual should realize its potential for social action, first of all, the benefits as well as its dangers. The main concept in relation to politics here is e-mobilization.[38] In an era of media creating a tool for political mobilization by providing information in an easy, cheap and convenient way, it is crucial for the development of networked political infrastructure to engage as much of the public as possible in participating in politics[39].

As cyberspace becomes a virtual reflection of physical reality, it is also penetrated by negative forms of human activity. The structure created for scientific cooperation of the Internet network provides a great sense of anonymity, and is used by criminals, terrorists, as well as some countries pursuing hostile policies in the global environment to carry out illegal activities or aggression against other entities. Nor can we forget the use of the media as a means for the attackers to spread disinformation in society. The growing activity of terrorists in cyberspace nowadays poses a very serious challenge, as launching a cyber attack is relatively easy and cheap for the attackers, but difficult for security actors to detect and can cause catastrophic consequences. Indeed, a smoothly executed attack can paralyze the functioning of public institutions even throughout the country and generate huge costs. It has already been emphasized many times that the media have a very strong impact on the psyche and attitudes of the public, especially in the context of terrorism. Two mechanisms are the most important in this regard: the first is manipulation of fear and manipulation of information.

Fake news has a negative impact on people's emotions, reasoning and behavior by creating a false picture of reality. Although disinformation is not a new phenomenon, the development of the Internet and social networks has made it possible to manipulate public opinion on an unprecedented scale. Creators of false information take advantage of certain imperfections of the human mind, mechanisms of influence and other phenomena described in psychology, to achieve political, financial, ideological or image goals. Understanding the psychological aspects

[38] J. Nowak „wykorzystywanie Internetu przez grupy interesu i ruchy społeczne do celów politycznej rekrutacji, organizacji i kampanii „*Aktywność obywateli online Teorie a praktyka*" WYDAWNICTWO UNIWERSYTETU MARII CURIE-SKŁODOWSKIEJ, LUBLIN 2011.

[39] Y. Benkler, R. Faris, H. Roberts, „Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics", OXFORD University Press, New York USA, 2018, p. 15-16.

of the impact of fake news on humans is the first step to building public resistance to disinformation[40].

In this struggle, disinformation and the imposition of emotional perceptions of reality serve to achieve the aggressor's intentions. Lack of control over manipulation is most often related to the subject's lack of knowledge of the phenomenon and awareness of being manipulated[41].

The digital revolution has defined the way communities communicate and obtain and share information. The media or advertising market has also been profoundly transformed. With this change, the phenomenon of misinformation has evolved. Socialmedia is now one of the key channels for distributing false content. Disinformation on the Internet cannot only affect democratic electoral processes or shape public opinion, but also cause serious financial losses in business[42].

The modern concept of "security" covers a much wider scope than in the past. This is because it refers to political, technical, economic, ecological aspects, military, social and humanitarian factors. Accordingly, we can consider security as a multidimensional category, referring to the individual, the state, international relations or characterizing the situation of any actor of social life.

One of the biggest challenges among the wide catalog of threats in the modern world is disinformation. This is a threat that is often impossible to detect, causing huge losses, resulting from the use by hostile environments of ever newer tools of modern technology using psychological actions, enabling action on an unlimited scale.

The international community's realization of the possible scale of threats arouses a natural need to build security. States interested in the common good of security are taking measures and actions to defend themselves against disinformation. Attention should be paid to the role of the media, which, using a wide range of means to spread information, can become a tool in the hands of aggressors and terrorists to spread widespread panic and fear. On the

[40] P. Zegarow, *„Dlaczego wierzymy w dezinformację? Analiza mechanizmów psychologicznych"*, [in:] M. Wrzosek, *„Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes"*, NASK Cyber POLICY, NASK Państwowy Instytut Badawczy, Warszawa 2019, p. 29.

[41] O. Wasiuta, S. Wasiuta, *„Wojna hybrydowa Rosji przeciwko Ukrainie"*, Arcana, Kraków 2017, p. 162–163; eidem, *„Medialna manipulacja informacją w wojnie hybrydowej Rosji przeciwko Ukrainie"*, [in:] *„Medialne obrazy świata. Wybrane problemy społeczno-polityczne w mediach"*, (ed.) R. Klepka, Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018.

[42] M. Wrzosek, *Zjawisko dezinformacji w dobie rewolucji cyfrowej. op. cit.*, s. 57.

other hand, the media are helpful in the fight against this phenomenon by publishing information about possible danger and ways to behave when the security of individuals
and groups is challenged. All the above-mentioned measures are designed to achieve the intended purpose, which is to determine the effects of media discourse on disinformation, projecting the sense of security of citizens.

In view of the above, the research conducted for this publication addressed the identification of respondents' awareness and attitudes toward the existence of fake news and disinformation on the Internet. The survey encompassed the following issues:

- the level of trust in news and information provided through various information channels;
- people's perception of how often they encounter news or information that is misleading or fake;
- public confidence in identifying news or information that is misleading or fake;
- respondents' view of the scale of the disinformation problem in cyberspace;
- the view of what institutions and media actors should do to stop the spread of fake news.

With regard to the level of trust in news and information provided through various information channels, respondents are less likely to trust news and information delivered through online sources (newspapers and online magazines) 43%, websites and podcasts 28% while social networks and instant messaging 29%. The vast majority of respondents completely trust or tend to completely trust news and information obtained through television channels 62%, while through radio 64%.

As for the respondents' perception of how often they encounter news or information that is misleading or false respondents in the group 41% said they encounter false information daily or almost daily, another 38% said it happens at least once a week.

Public confidence in identifying news or information that is misleading or false - 65% of respondents say they are completely or somewhat confident in their ability to identify news or information that misrepresents reality. In contrast, 32% of respondents are unsure or unable to identify news or information when it comes to identifying it.

The vast majority of respondents,i.e. as many as 88% with regard to the scale of the problem of disinformation in cyberspace, believe that the phenomenon of disinformation on the Internet is a huge problem that definitely affects the mood of citizens. Similarly, 86% of respondents believe that it is a serious problem that threatens the security and democracy of the country.

Regarding respondents' opinion and view of what institutions and media actors should take action to stop the spread of fake news and information, respondents indicated journalists - 51%, followed by state institutions and offices - 42%, social networks - 34%, EU institutions - 29%, and NGOs received an indication of 31%.

CONCLUSION

States must redefine the role of the media in order to conduct an effective fight against disinformation. As a means of communication, the media should provide reliable information about the events that have occurred and how citizens should behave in a particular situation.

An important element in the fight against disinformation also includes the development of a media policy and a strategy for cooperation between the government and the mass media, which will allow joint efforts to combat disinformation and reduce its social impact. One should also not forget the need to intensify efforts on the Internet, especially social media. Those responsible for ensuring security in the country should conduct propaganda and educational campaigns using the World Wide Web, as they can have positive effects in reducing the public sense of threat and fear of, for example, military, economic or terrorist threats.

The outcomes of the analysis of the conducted research related to disinformation in the broad sense of online security, confirm the fact that even traditional mass media have a negative impact on the level of security perceived by citizens. This is because content on the Internet is based mainly on the publication of articles that arouse sensations, and such are undeniably military actions, the global economic situation, the state of epidemics or terrorist attacks. The disseminated materials are aimed at a wide audience and strongly influence its worldview. Despite the fact that a significant part of them perform informational and educational functions, they largely play propaganda roles and affect the reader's emotions. Among the titles analyzed, the vast majority can be categorized as journalism. They are suggestive in nature and direct the reader to the authors' desired course of thought. In the same way, their content is constructed, which, in a threatening situation of, among other things, an attack of a military, pandemic or terrorist nature, incites anxiety and fear in society, and shapes public opinion in a particular way desired by the sender.

In the modern world, disinformation is an extremely dynamic phenomenon. It undergoes constant changes under the influence of scientific and technological progress and civilization development.

Such a situation should not be underestimated, especially at a time when the activities of terrorists are focused on a broad communication strategy aimed at disinforming societies regionally and globally.

An increasing percentage of respondents declare a personal sense of insecurity and a conviction that the country is insufficiently prepared to combat disinformation.

The use of selected research methods and techniques, which were the analysis of the content of the literature and own research, contributed to the achievement of the purpose of this publication. It also succeeded in answering the main research question.

An element necessary for the proper analysis of the problem was also to answer the specific questions. Verification of the collected materials shows that the media in the 21st century are moving away from performing their primary function, which is to reliably inform the public and show the entire spectrum of events, in favor of the strongest possible influence on the audience and the formation of their opinions. According to respondents, another not inconsiderable factor motivating the media to act is the desire to make above-average profits. A consequence of this state of affairs is the continued decline in the trust of Polish audiences in the mass media, and consequently, their involvement in individual analysis of content published mainly on the Internet is increasing.

Interpretation of the collected materials confirmed that mass media have a very strong impact on the level of feeling of security among citizens.

The impact of content posted on the Internet on public awareness is evidenced, among other things, predominantly through publications referring to the phenomenon of the threat of war, epidemics and growing terrorism, used the appeal to emotions.

However, it should be noted that the media can contribute to the fight against the phenomenon in question. Educating the public and building journalistic ethics is crucial. The issue of developing a strategy for joint action by the media and public authorities to effectively level the threat of the phenomenon of disinformation in the mass media should also not be overlooked.

In conclusion, the analysis and interpretation of the collected research material made it possible to confirm the veracity of the hypothesis formulated at the beginning, according to which the discourse of the phenomenon of disinformation contributes to the creation of a sense of threat and arousal of social unrest.

The fear of the phenomenon of disinformation is nowadays a permanent element of everyday life, so the priority is to develop new methods and strategies aimed at neutralizing the phenomenon in question.

Certainly, this publication does not exhaust such a complex subject as disinformation in the age of the digital revolution in terms of state security. It is only an attempt to make a comprehensive analysis in relation to a certain part of social reality. A significant number of the threads raised in this publication requires deeper analysis and further research.

REFERENCE LIST

(MINI) Słownik BBN - Propozycje nowych terminów, https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html

Aiken A., RESIST Counter-disinformation toolkit, RESIST 2 Counter Disinformation Toolkit - GCS (civilservice.gov.uk).

Benkler Y., Faris R., Roberts H., Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics, OXFORD University Press, New York USA, 2018.

Grabowska-Lepczak I., Kwiatkowski M., Tryboń M., Bezpieczeństwo człowieka w obliczu XXI wieku, Zeszyty Naukowe Szkoły Głównej Służby Pożarniczej, no 41/2011, Warszawa 2011.

Gracik M., K. Żukowska K., Bezpieczeństwo międzynarodowe. Teoria i praktyka, Szkoła Główna Handlowa, Warszawa 2006.

JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Action Plan against Disinformation, Brusseles.

Kaczmarek J., Skowroński A., Bezpieczeństwo Świat – Europa - Polska, Wrocław, 1998.

Koziej S., Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja, Warszawa, 2011.

Kula H. M., Propaganda współczesna. Istota – właściwości, Wydawnictwo Adam Marszałek, Toruń 2005.

Kwiecińska M., Wykorzystanie mediów dla podniesienia bezpieczeństwa, potrzeby i sposoby realizacji, Obronność. Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia, no 3/2014, Akademia Obrony Narodowej, Warszawa 2014.

Modrzejewski Z., Operacje Informacyjne, AON, Warszawa 2015.

NATO Strategic Communications Policy, https://publicintelligence.net/nato-stratcom-policy

Nowak J. Wykorzystywanie Internetu przez grupy interesu i ruchy społeczne do celów politycznej rekrutacji, organizacji i kampanii [w:] Aktywność obywateli online Teorie a praktyka, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2011.

Piertaś Z. J., Podstawy teorii stosunków międzynarodowych, Uniwersytet Marii Curie-Skłodowskiej, Lublin 1986.

Potejko P., Bezpieczeństwo informacyjne, [in:] Bezpieczeństwo państwa, K.Wojtaszczyk, Materska-Sosnowska A., (ed.), Oficyna Wydawnicza ASPRA-JR, Warszawa 2009.

Rada Europejska, Sekretariat Generalny Rady, Posiedzenie Rady Europejskiej (19 i 20 marca 2015 r.) – Konkluzje, Bruksela.

Raport „Freedom on the Net 2017. Manipulating Social Media to Undermine Democracy", https://freedomhouse.org/report/freedom-net/freedom-net-2017.

Rokiciński K., Pac B., Operacje informacyjne w działaniach militarnych, Wydawnictwo J.P., Gdynia 2010.

Strategic Communication Joint Integrating Concept, http://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/jic_strategiccommunications.pdf?ver=2017-12-28-162005-353

Szopa T., Koncepcja graficznego przedstawiania terytorialnego rozkładu ryzyka i zagrożeń, [in:] J. Wolanin (ed.) Mapy terytorialnego rozkładu ryzyka, Wydawnictwo EDURA, Warszawa 2004.

Wasiuta O., Wasiuta S., Wojna hybrydowa Rosji przeciwko Ukrainie, Arcana, Kraków 2017; eidem, Medialna manipulacja informacją w wojnie hybrydowej Rosji przeciwko Ukrainie, [in:] Medialne obrazy świata. Wybrane problemy społeczno-polityczne w mediach, Klepka R (ed.), Wydawnictwo Naukowe Uniwersytetu Pedagogicznego, Kraków 2018.

Wilbur D., Propaganda's Place in Strategic Communication: theCase of ISIL's Dabiq Magazine, „International Journal of Strategic Communication" 2017, Vol. 11., No. 3.

Wrzosek M., Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, NASK Cyber POLICY, NASK Państwowy Instytut Badawczy, Warszawa 2019.

Zdrodowski B., Istota bezpieczeństwa państwa., Wyższa Szkoła Policji w Szczytnie, Istota bezpieczeństwa państwa (up.krakow.pl).

Zegarow P., Dlaczego wierzymy w dezinformację? Analiza mechanizmów psychologicznych, [in:] Wrzosek M., Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, NASK Cyber POLICY, NASK Państwowy Instytut Badawczy, Warszawa 2019.

Zięba R., „Pojęcie i istota bezpieczeństwa państwa w stosunkach międzynarodowych, „Sprawy międzynarodowe", no. 10/1989, Polski Instytut Spraw Międzynarodowych, Warszawa 1989.