SECURITY DIMENSIONS
NO. 37; 2021 (66–75)
DOI 10.5604/01.3001.0015.3293

Threats to State Security in the Aspect of Disinformation

Tomasz Dukiewicz[*]

ABSTRACT

Information in the aspect of security plays a significant role in influencing the spectrum of the functioning of the state. In today's information chaos, information has become a tool of manipulation and disinformation, also used in the implementation of strategic goals of a given country. States can thus achieve their strategic goals because it is less costly, more difficult to detect, and allows some sort of manipulation of the rationale behind such actions. Such countries include countries for which democracy is only a concept. It can be indicated that information is a raw material that, in the process of manipulation and disinformation, becomes a kind of a tool that can be used in a targeted way. The issue of fighting disinformation is of key importance today.

ARTICLE INFO

Article history
Received: 07.07.2021 Accepted: 12.07.2021

[*] Tomasz Dukiewicz, PhD, ORCID: 0000-0001-7833-9619, University of Opole, Faculty of Law and Administration, Opole, Poland; correspondence address: ul. Katowicka 87a, 45-060, Opole, Poland; e-mail: tdukiewicz@uni.opole.pl

Keywords
disinformation, manipulation, propaganda, security environment

Introduction

The growing ambitions of some actors bordering Poland (Russia, Belarus), ready to use armed force or the threat of using it to promote their interests, primarily affect the stability of the state's security. Russia's actions in the political and military field with regard to the international environment, as well as the Kremlin's readiness to introduce conflict situations, taking into account losses and gains, show the adopted strategy, the tool of which is, inter alia, the use of information operations.

Provoked intelligence, migration or border incidents can serve as a cover and tool for information activities. Russian disinformation is the glue that binds actions across a broad spectrum of threats. Active means of informing influence include intelligence, military, diplomatic, media, cyber, social, economic and financial activities. It is the incidents related to the above-mentioned dimension that constitute the strategic source of achieving the strategic goals of the Russian Federation. The activities are carried out with the use of means of influence creating the image of "bad west in relation to an innocent, good Russia." Aspirations of these actors are associated with a significant increase in their military capacity, including offensive cyber-weapons, weapons of mass destruction and measures for its transfer, growing demand for key raw materials, financial market activity, competition for influence in strategic areas and more aggressive distribution of their political ambitions on international forums.[1]

One-sided attempts by some countries to build spheres of influence by combining political, economic and military pressures and intelligence activities can be considered a threat, and these pressures and actions are also used in cyberspace. These factors are related to the progressive erosion of political and legal obligations for European security. The threats to security come largely from weak or failed states whose governments are unable to defend themselves, the security of citizens, and the rule of law. As a result, there are national and regional conflicts that negatively affect external security.

[1] J. Darczewska, P. Zachowski, 'Nie tylko dezinformacja – przyczynek do analizy rosyjskiego zagrożenia' [report], in: *Zjawisko dezinformacji w dobie rewolucji cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes*, Warszawa, NASK Państwowy Instytut Badawczy, 2019, pp. 51–52, https://cyberpolicy.nask.pl/wp-content/uploads/2019/09/Raport_CP_Dezinformacja_ONLINE_s.pdf (accessed 8 July 2021).

Threats Used in Disinformation Activities

Security in the face of challenges is unlimited, while in the spectrum of internal threats to the state and in the area of external threats, these are two types of security that are similar to each other, but completely different in their structure. When describing an external threat, it can be stated that it is a form of threat connected directly or indirectly with the probability of a threat related to the inviolability of Poland's territory or the limitation of our state sovereignty to a party to the conflict. This threat is directly related to the activities of another state for the benefit of civil freedom and the inviolability of borders.[2]

On the other hand, the internal security of the state includes the state of stability and guarantees the development of society. In order to be able to speak of a sense of security, there must be no threats to the functioning of the systems of state organs. Internal security also includes state institutions and bodies (along with private entities) whose task is to protect the stability and integrity of the state, and which are characterized by a constant readiness to act.

The growing severity of non-military threats (e.g., energy, migration, cyber-attacks, information operations) and the deteriorating security situation in areas directly adjacent to NATO and EU Member States make Europe increasingly demanding on its ability to react independently and highlight gaps in its capabilities and security readiness to fend off threats.

The negative aspects of the globalization process include the possibility of abusing the interconnectedness of financial markets in the absence of an effective system of international regulations, and the abuse of information and communication infrastructure and technology. Uneven economic development and the easy spread of radical political, populist and religious ideas also contribute to instability.[3]

One of the consequences of current events in the world economy may be a change in the relative importance of individual actors, including the possible weakening of Europe and the US, and the continued tendency of states to override national interests at the expense of com-

[2] Z. Polcikiewicz, P. Siemiatkowski, P. Tomaszewski (eds.), *Współczesne wyzwania polityki bezpieczeństwa państwa*, Toruń, Towarzystwo Organizacji i Kierownictwa Dom Organizatora, 2019, p. 23, DOI: 10.5281/zenodo.3244158

[3] Oxford Analytica, 'Global Trends to 2035', *Oxan.com*, September 2017, global-trends-to-2035-geopolitics-and-power.pdf, (accessed 6 January 2021).

mon interests, and other possible trends that may reduce NATO and EU solidarity and effectiveness.

Compared to states and international organizations, non-state actors can make faster and more flexible use of the opportunities offered by globalization, in particular the integration of ICT, transport and trade. The position of states as entities with a monopoly on the use of force and regulators of key economic and information flows is declining in importance. On the contrary, the ability of non-state actors to threaten the interests of states, replace elements of the state system with their own structures, implement territorial ambitions and, using extreme violence, threaten the safety of the population and the stability and integrity of the affected states.

The security implications of demographic change will continue to increase, the risk of an ageing population in developed countries and uncontrolled migration.

Problems related to poverty, long-term social exclusion and the lack of basic needs and services can significantly increase the likelihood of extremism, crime, local armed conflict and mass and uncontrolled migration.[4]

Increasing dependence on the availability of natural resources leads to increased global competition in access to strategic raw materials and energy. The importance of the protection of critical infrastructure is growing, and above all the means of transport of strategic raw materials, which are characterized by a high degree of susceptibility to potential state and non-state entities.[5]

The effects of climate change on human health and the environment are now a reality. However, the fear of this change itself may lead to increasing tensions between states, resulting in a humanitarian crisis with direct consequences for local, state and international structures, including the possible escalation of local conflicts along with increasing migratory pressure.[6]

[4] European Commission, 'European Commission Report on the Impact of Demographic Change' [report], *An official website of the European Union*, https://ec.europa.eu/info/sites/default/files/demography_report_2020_n.pdf, (accessed 6 January 2021).

[5] National Intelligence Council, 'Natural Resources in 2020, 2030, and 2040: Implications for the United States', *Office of the Director of National Intelligence*, 25 July 2013, https://www.dni.gov/files/documents/NICR%202013-05%20US%20Nat%20Resources%202020,%202030%202040.pdf, (accessed: 6 January 2021).

[6] C.E. Werrell, F. Femia, 'Climate change raises concerns about conflict', *UNESCO*, https://en.unesco.org/courier/2018-2/climate-change-raises-conflict-concerns, (accessed 6 January 2021).

Disinformation turns out to be an extremely dangerous element of a fight between, for example, rival companies. They can also be used during a pandemic to destabilize the state and its security, e.g. by providing incorrect information about the virus, its functioning and prevention. It is important to carefully search for and eliminate possible efforts leading to the falsification of information, especially that stored in public databases, which may also be accessed by dishonest users.[7]

Disinformation Environment

The dynamics of events in the Polish security environment is today the greatest since the collapse of the Soviet Union. The Russian government does not really hide the goals of information warfare.

The Russian Federation, using information warfare, is ready to destabilize the situation in other states and undermine their territorial integrity, while openly violating international law. Its activities are often masked and carried out below the threshold of war. It should be considered to what extent is the real action of Russia which initiates a conflict on a regional scale involving one or more NATO member states. Observing the Russian superpower policy, it cannot be ruled out that proxy conflicts will arise in various parts of the world in order to create new fields of pressure on Western countries. Russian policy is closely coordinated with the actions of secret services, including active actions (e.g. disinformation) towards other countries.

Social trends such as populism and rising tensions caused by disinformation in societies less and less resilient to their influence can trigger crises over time that require international support.[8]

Following the words of Nobel Laureate Paul Romer, who said that the crisis is a terrible phenomenon to waste. The crises to date indicate that they have been wasted as an opportunity to achieve balance in many dimensions affecting security. Crises reveal weaknesses in terms of multidimensional impact. When observing faster and faster changes, not only political but also military, economic, social and cultural, it should be considered that they constitute an important source of disinformation activities influencing the

[7] EU Council, 'Disinformation during the COVID-19 pandemic', *Consilium*, 23 July 2020, https://www.consilium.europa.eu/pl/documents-publications/library/library-blog/posts/disinformation-during-the-covid-19-pandemic/, (accessed 6 January 2021).

[8] 'Fostering Economic Resilience in a World of Open and Integrated Markets', *OECD*, https://www.oecd.org/newsroom/OECD-G7-Report-Fostering-Economic-Resilience-in-a-World-of-Open-and-Integrated-Markets.pdf, (accessed 6 January 2021).

security environment. The gap between reality, truth and the fragmented reality, which is the disinformation necessary for the formation of an alternative reality, becomes more and more visible. In view of the growing importance of information, the negative approach to information security is insufficient to ensure national security.[9]

The complete dependence of the public and private sphere on information and communication technologies increases the severity of the effects in the most important pillars of the state's functioning. Analysing the above thesis, one should expect a proportional increase in threats in relation to the stability of security.

Disinforming recipients is easier when using special services, social networks, media, conferences, celebrations, etc. However, sometimes disinformation of a person who informally leads a large social group may turn out to be a better and less costly solution. It is assumed that a citizen of a country is a target whose social position or abilities allow him to manipulate and disinform or influence society.[10]

The disinformer may be recruited by the services of a hostile state. After the delivery of certain informational content, it is most likely disseminated because it comes from a person with social trust. After all, disinformation is based on human emotions, incompetence, credulity and lack of situational imagination, and these are global and timeless, hence the high effectiveness of disinformation activities.

Disinformation takes advantage of the limited possibilities and capabilities of analysing and verifying information, gaining a temporary advantage. The characteristics of contemporary disinformation should be seen in a broader context. Time is an important determinant of disinformation activities. Depending on the scale of disinformation, time will be different in relation to a specific recipient (MP, government, social group, state, etc.) It is worth mentioning that democracy is based on the fundamental foundation of freedom of speech, which also creates space for disinformation activities. Searching for a solution to this dilemma is not easy. We are dealing

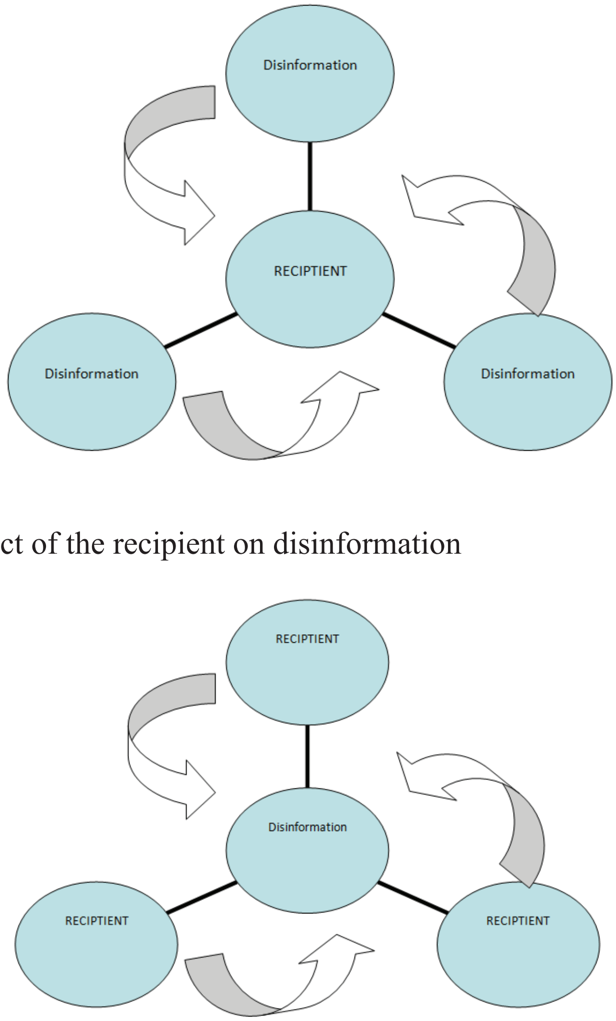
[9] J. Bayer et al., 'Disinformation and propaganda – impact on the functioning of the rule of law in the EU and its Member States', European Parliament, February 2019, https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608864/IPOL_STU(2019)608864_EN.pdf, (accessed 6 January 2021).

[10] T. Dukiewicz , 'Disinformation as a hidden tool of influence environment', *Security Forum 2020*, Slovakia, Interpolis, Matej Bel University in Banská Bystrica, 2020, p. 47, ISBN 978-80-973394-3-2G.

here with something that can be described as a basic dilemma of modern democracy. A quick response to disinformation gives a chance to reduce its effectiveness in terms of the intended purpose of the impact.

Fig. 1. Dependence of the Impact of Disinformation

a) The impact of disinformation on the recipient



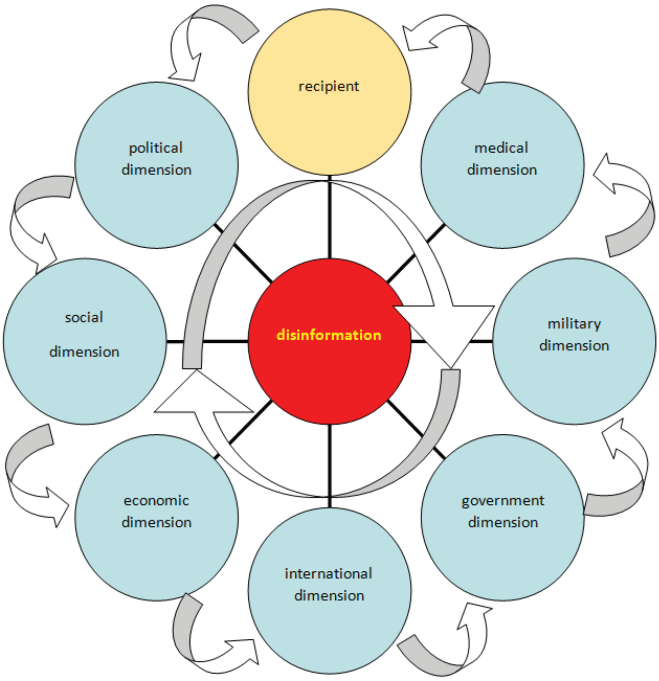
b) The impact of the recipient on disinformation

Source: Own study.

The impact of disinformation should be perceived not only by taking into account the direct recipient, but also the environment that will indirectly be or is a participant in these activities. The essence of preventing the scale of disinformation serving to manipulate a specific audience is the quick presentation of facts. If the scope of disinformation affects not only a specific recipient, the indirect goal of disinformation, as shown by scientific research, will be achieved. When analysing the features of disinformation, it can be concluded that it should theoretically contradict the features of useful information.

However, in order to implement effective disinformation, information often needs to be relevant, including reaching the right audience. In selected disinformation activities, disinformation will be updated in order to authenticate the content. Depending on the needs of disinformation activities, the information utility features can be selected and freely transformed in order to achieve the chosen goal. In this way, disinformation can take control or be contrasted with any useful information.

Fig. 2. Diagram of the Impact of Disinformation on the Environment



Source: Own study.

Misinforming the recipients is easier when special services, social media, mass media, celebrations (etc.) are used. However, sometimes disinformation of a person with informal leadership in a large social group may be a better and less costly solution. It is assumed that a citizen of a country a target whose social position or abilities enable him/her to misinform compatriots or influence them, can be recruited by a state intelligence officer who provides disinformation. Once certain information content is transferred, it is very likely to be spread as it comes from a person with social trust. After all, disinformation is based on human emotions, incompetence, credulity, and lack of situational imagination – and these are global and timeless, hence the effectiveness of disinformation operations.

Conclusions

By using today's technology to conduct disinformation activities in the face of the internal and external security challenges of the state, it is possible to learn the expectations and concerns of social groups, which allows to define a disinformation strategy. The effectiveness of disinformation depends not only on coordination within the initiating structures, but also on the awareness of recipients and the readiness to counteract state structures. Therefore, in disinformation, it is pointless to provide data that not only will not confuse, but may even raise objections and doubts about the credibility of the source.

During the prevailing COVID-19 pandemic, we may see an increase in public interest in the threats of disinformation, the effects of which are used to achieve any goal. A similar example of an attempt at disinformation of public opinion also in the international environment can be seen in the example of the migration conflict inspired by Belarus and Russia. Research shows that awareness of the problem is still insufficient to effectively protect against the impact of disinformation. Given the features of disinformation, the fight against disinformation remains extremely difficult. Despite the emerging institutions at the national and international level that counteract disinformation, a large part of the society still succumbs to it. In order to properly and effectively fight disinformation, it is necessary to increase the awareness and knowledge of the society, as well as to deepen research and devote more time to a proper understanding of the mechanisms and techniques used in disinformation activities that affect state security.

References

1. Werrell, C.E., Femia, F., 'Climate change raises concerns about conflict', UNESCO, https://en.unesco.org/courier/2018-2/climate-change-raises-conflict-concerns, (accessed 6 January 2021).
2. Darczewska, J., Zachowski, P., 'Nie tylko dezinformacja – przyczynek do analizy rosyjskiego zagrożenia', in: *Zjawisko dezinformacji w dobie rewolucji*

cyfrowej. Państwo. Społeczeństwo. Polityka. Biznes, Warszawa, pp. 51–52, NASK Państwowy Instytut Badawczy, 2019.

3. Bayer, J. et al., 'Disinformation and propaganda: impact on the functioning of the rule of law and democratic processes in the EU and its Member States', *European Parliament*, February 2019, https://europarl.europa.eu/RegData/etudes/STUD/2021/653633/EXPO_STU(2021)653633_EN.pdf, (accessed 6 January 2021).
4. EU Council, 'Disinformation during the COVID-19 pandemic', *Consilium*, 23 July 2020, https://www.consilium.europa.eu/pl/documents-publications/library/library-blog/posts/disinformation-during-the-covid-19-pandemic/, (accessed 6 January 2021).
5. Dukiewicz, T., 'Disinformation as a hidden tool of influence environment', *Security Forum 2020*, Slovakia, Interpolis, Matej Bel University in Banská Bystrica, 2020, p. 47, ISBN 978-80-973394-3-2
6. European Commission, 'European Commission Report on the Impact of Demographic Change' [report], *An official website of the European Union*, https://ec.europa.eu/info/sites/default/files/demography_report_2020_n.pdf, (accessed 6 January 2021).
7. Oxford Analytica, 'Global Trends to 2035', *Oxan.com*, September 2017, global-trends-to-2035-geopolitics-and-power.pdf, (accessed 6 January 2021).
8. National Intelligence Council, 'Natural Resources in 2020, 2030, and 2040: Implications for the United States', *Office of the Director of National Intelligence*, 25 July 2013, https://www.dni.gov/files/documents/NICR%202013-05%20US%20Nat%20Resources%202020,%202030%202040.pdf, (accessed 6 January 2021).
9. Polcikiewicz, Z., Siemiatkowski, P., Tomaszewski, P. (eds.), *Współczesne wyzwania polityki bezpieczeństwa państwa*, Towarzystwo Organizacji i Kierownictwa „Dom Organizatora”, 2019, p. 23, DOI: 10.5281/zenodo.3244158

Cite this article as:

T. Dukiewicz, “Threats to State Security in the Aspect of Disinformation”, *Security Dimensions*, no. 37, 2021, pp. 66–75, DOI 10.5604/01.3001.0015.3293.