

# Information Security Policy

Conditions, Threats and Implementation  
in the International Environment



EDITED BY  
PIOTR BAJOR



# **INFORMATION SECURITY POLICY**



# **INFORMATION SECURITY POLICY**

**Conditions, Threats and Implementation  
in the International Environment**

**edited by  
PIOTR BAJOR**



**Kraków 2022**

© Copyright by individual authors, 2022

Piotr Bajor

Jagiellonian University in Kraków, Poland

 <https://orcid.org/0000-0003-2569-2552>

 [piotr.bajor@uj.edu.pl](mailto:piotr.bajor@uj.edu.pl)

Review: Marek Delong

Language editor:

Cover design: Marta Jaszczuk

ISBN 978-83-8138-826-9 (print)

ISBN 978-83-8138-827-6 (PDF)

<https://doi.org/10.12797/9788381388276>

The publication is available under the Creative Commons Attribution 4.0 International license. Some rights reserved by the authors. The publication was created as part of the “Public Diplomacy 2022” competition. Any use of the work is allowed, provided that the above information is preserved, including information about the license used and about the rights holders.

The opinions expressed in this publication are those of the authors and do not reflect the views of the official positions of the Ministry of Foreign Affairs of the Republic of Poland.



---

Ministry  
of Foreign Affairs  
Republic of Poland

Public task financed by the Ministry of Foreign Affairs of the Republic of Poland within the grant competition “Public Diplomacy 2022”.



The project was implemented by the Foundation Center for Research on the Contemporary Security Environment, in cooperation with a research team from the Jagiellonian University in Kraków.

KSIĘGARNIA AKADEMICKA PUBLISHING

ul. św. Anny 6, 31-008 Kraków

tel.: 12 421-13-87; 12 431-27-43

e-mail: [publishing@akademicka.pl](mailto:publishing@akademicka.pl)

<https://akademicka.pl>

# Table of contents

Introduction .....	7
MAGDALENA DANEK Social Media as a Recipient and Creator of Political Actions in the Context of the Security Crisis.....	9
AGNIESZKA NITSZKE The European Union versus Russian Disinformation .....	35
MICHAŁ MAREK Information Security and Mechanisms Used by the Russian Federation to Shape Polish Public Opinion.....	53
MONIKA ŚLUFIŃSKA The Russia-Ukraine War. Two Strategies of Communication? .....	67
ADRIAN TYSZKIEWICZ The Russian Narrative Construct towards Ukraine.....	83
PIOTR BAJOR Information Security Policy of Ukraine – Assumptions and Effectiveness .....	99
Index of names .....	123



# Introduction

This publication discusses issues related to information security, analysed through the lens of considerations, threats and implementation policies. The publication is the result of studies done by the research team implementing a project related to information security as part of the “Public Diplomacy 2022” competition organised by the Polish Ministry of Foreign affairs; according to rules of the competition, papers published as part of the contest constitute results of original research and do not reflect the official stance of the Ministry.

Information security is one the key aspects of modern security and its importance has been significantly increasing in contemporary international relations. This publication presents the results of studies on several key aspects related to this issue. The publication contains results of research on considerations related to information security, related threats and its implementation, as well as research on social media, analysed through the lens of the object and subject of disinformation activities. This aspect includes an analysis of communication strategies adopted in respect of the Russian aggression and the ongoing war between Russia and Ukraine, as well as mechanisms implemented as part of information security policies to shape public opinion. The publication also presents results of research directly concerning Ukraine’s information security policy, analysed from the point of view of its tenets and implementation in successive years, EU’s policy aimed at combating Russian disinformation, and presents an analysis of Russian narratives on Ukraine against the backdrop of wider geopolitical and international considerations.

The perspective presented in the publication concerns selected aspects that make up the concept of security, analysed from the point of view of theoretical assumption, as well as their importance for contemporary analysis of information security and related considerations and threats. The objective of this publication was therefore to present the latest results of research into the issues mentioned above, as well as to deepen the discussion on both theoretical and practical aspects of information security which has become an extremely significant issue in today’s world.

Piotr Bajor



MAGDALENA DANEK 

*Jagiellonian University in Kraków*

## Social Media as a Recipient and Creator of Political Actions in the Context of the Security Crisis

**ABSTRACT:** Social media is not only an increasingly popular communication channel or business tool, but also one of the arsenals of information warfare. The next phase of Russia's war against Ukraine, launched on February 24, 2022, showed once again that the content disseminated through it is used not only to provide actual information or to improve the organisation of assistance to refugees, but also to spread disinformation and propaganda. The aim of the article is to analyse the current status of social media platforms as tools of influence and power – particularly during the war in Ukraine – as well as activities aimed at combating disinformation, especially in the context of the activities of the EU, selected state actors and the owners of these platforms themselves (in this aspect, the analysis will include the activities of Meta and Twitter). The research hypothesis is based on the assumption that social media is, in the scope of the present issue, not only the recipient of political decisions made by legitimised actors, but – by virtue of their power over the flow of a significant amount of information – it become an important actor in these activities in terms of influencing political processes and decision-making centres (e.g., by

arbitrarily deciding on the visibility of hate speech content in situations of armed conflict).

KEYWORDS: social media, disinformation, Ukraine, power, influence, hybrid war

## Introduction

With the emergence and development of the internet and the applications based on it, including social media, expectations could be seen in both public and academic discourse about the opportunity to make them tools to strengthen democratic processes and political engagement of citizens. Thus, television, which Robert Putnam saw as one of the main causes of generating civic passivity and the erosion of social capital,<sup>1</sup> was to give way to an egalitarian and interactive space based on free access to information and free expression of opinion. Jan van Dijk concludes that hopes for the impact of ICT on politics were linked primarily to increasing the acquisition and exchange of information between government and administrative representatives and citizens, enhancing public debate, deliberation, the formation of communities and citizen participation in decisions of public importance.<sup>2</sup> These approaches were based on the belief that increasing citizens' access to information benefits both society itself and democratic procedures.

The massive proliferation of false content on social media, including the notorious disinformation campaigns accompanying events of particular significance – such as the 2016 US presidential election, the campaign for Britain's exit from the European Union (EU), the COVID-19 pandemic or the next round of the war in Ukraine launched on February 24, 2022 – are shifting the focus towards seeing the internet and the applications that function within it as a space not primarily for debate, but information warfare.<sup>3</sup>

---

<sup>1</sup> R. Putnam, *Samotna gra w kręgle. Upadek i odrodzenie wspólnot lokalnych w Stanach Zjednoczonych*, transl. P. Sadura, S. Szymański, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008, p. 384.

<sup>2</sup> J. van Dijk, *Społeczne aspekty nowych mediów*, transl. J. Konieczny, Wydawnictwo Naukowe PWN, Warszawa 2010, p. 150.

<sup>3</sup> A. Guess, B. Nyhan, J. Reifler, *Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 US Presidential Campaign*, 9.01.2018, [on-line:] <https://about.fb.com/wp-content/uploads/2018/01/fake-news-2016.pdf>, 20 November 2022; M.T. Bastos, D. Mercea, "The Brexit Botnet and User-generated Hyperpartisan News", *Social Science Computer Review*, vol. 37, no. 1 (2019), pp. 38–54; Y.M. Rocha et al., "The Impact of Fake News on Social Media and Its Influence on Health during the COVID-19 Pandemic: A Systematic Review", *Journal of Public Health* (2021), pp. 1–10.

The information space has, since ancient times, been seen as a vital pillar of security and, at the same time, a tool for confrontational action. This is expressed in the words of Sun Tzu, who – in his treatises – indicated that *war is about being misled*.<sup>4</sup> Coherent management of the information space, especially in its digital dimension, is one of the key elements of state security.

The approach to war as not only a kinetic clash, but a whole range of diverse actions – including a special role for the information sphere – has been particularly popularised in the context of the notion of hybrid warfare. The clearest emanation of this phenomenon was Russia's actions towards Ukraine with the annexation of Crimea and the start of fighting in the Donbas region in 2014. The Russian Federation's point of view on the modern battlefield can be reconstructed from an article by the Chief of the General Staff of the Russian Armed Forces (Valery Gerasimov), where he states that nowadays, the fundamental principles of war have changed, and the role of non-military means of achieving political and strategic goals has significantly increased – often exceeding the power and effectiveness of kinetic weapons.<sup>5</sup>

In this sense, hybrid warfare, also referred to as *a war of controlled chaos*, encompasses the entire range of actions implemented to destabilise the economic and political situation, disintegrate and limit sovereignty, and consequently change political power to that controlled by the aggressor.<sup>6</sup> Although the concept of hybrid warfare does not have a clearly defined scope of meaning – and, thus, faces accusations of blurring the boundaries between times of war and times of peace, lowering preparedness for an appropriate response – it is noted that it points to key current and future security and defence challenges.<sup>7</sup>

Russia's ongoing war against Ukraine, which has been continuing since February 24, 2022, despite being – in its significant dimension – an example of a kinetic type of clash, is also marked by a meaningful potential for other acts with the hallmarks of a hybrid impact. It should be emphasized that, they are targeted not only at Ukraine,

---

<sup>4</sup> Sun Tzu, *Sztuka wojny*, transl. J. Zawadzki, Hachette, Warszawa 2009, p. 31.

<sup>5</sup> V. Gerasimov, "The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", *Military Review* (2016), [on-line:] [https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview\\_20160228\\_art008.pdf](https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf), 22 November 2022.

<sup>6</sup> O. Wasiuta, "Geneza pojęcia i zmiany podejścia do wojny hybrydowej w zachodnim dyskursie politycznym i wojskowym", *Przegląd Geopolityczny*, no. 17 (2016), p. 28.

<sup>7</sup> A. Bilal, "Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote", *NATO Review* 2021, [on-line:] <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.htm> (20.11.2022).

but also at Western countries. They manifest themselves, among other means, in large-scale propaganda actions or economic blackmail related to access to energy resources.

The aim of the article is to analyse the current status of social media platforms as tools of influence and the space of power making, in particular during the war in Ukraine, as well as activities aimed at combating disinformation – especially in the context of the activity of the EU, selected state actors and the owners of these platforms themselves (in this aspect, the analysis will include Meta and Twitter activities). The theoretical framework for the undertaken research will be the concept of the network society, and power understood as an influence on the management of communication processes by Manuel Castells. The research hypothesis is based on the assumption that in the scope of this issue, social media is not only the recipient of political decisions made by legitimate actors, but thanks to their control over the flow of a significant amount of information, they become an important actor of these activities in terms of influencing political processes.

In the course of the analysis carried out, three key reference levels were distinguished. The first relates to using social media as a new and increasingly crucial war arsenal in information warfare. The second one concerns regulatory action and the pressure exerted by political actors such as states and international organisations on social media platforms, which resultantly become the object of political action – especially in the context of the fight against disinformation. The last, but extremely important, dimension covers actions taken in relation to the conflict by the managers of social platforms, making them important actors of decision and political impact.

## Information management in cyberspace as an emanation of power

Manuel Castells, analysing the contemporary transformations of social, economic and political structures in the era of dynamic ICT development, introduces the concept of a network society (i.e., social structure) whose main features are the presence of digital network communication technologies, as well as the reproduction and institutionalisation of the connections created thanks to them through society itself. In this way, according to the researcher, a *new social morphology* is being created.<sup>8</sup> One of the essential dimensions of this emerging social structure are the power relationships

---

<sup>8</sup> M. Castells, *Spółczesność sieci*, crowd. M. Marody et al., transl. M. Marody, Wydawnictwo Naukowe PWN, Warszawa 2011, p. 491.

that are *exercised primarily by constructing meanings in people's minds*.<sup>9</sup> This approach reflects the concept of power as invisible, circulating, devoid of a specific location and, at the same time, omnipresent (as presented by Michel Foucault in his works).<sup>10</sup> For Castells, this process takes place via multimodal networks, where the type of communication appropriate for the era of new media is implemented. He describes this as *mass self-communication*.<sup>11</sup> Its essence is a potentially opposing combination of the global possibility of spreading messages with individualised and independent creation and reception based on personal selection.

Power, meaning a relational connection based on exerting influence, thus shifts in a network society from using physical violence to constructing meanings and media narratives. This process occurs mainly in communication networks assuming the role of new power centres. From this point of view, new media is not just neutral technical creations; access to them and the ability to use their networked architecture is one of the main sources of power. Under the concept of Castell, the nation-state coexists as one of the many sources of power and authority. At the same time, it is a node of a deeper network of power which consists of forces of capital, communication, international institutions, social movements, terrorist organisations, as well as local and regional authorities.<sup>12</sup> Due to the dynamic development and ubiquity of new media, the space of political competition is dominated by the media, which is becoming *the privileged realm of politics*.<sup>13</sup>

Therefore, in this sense, social media is not only platforms for the mass dissemination of information, but also active subjects for the exercise of power and influence (i.e., political actions), which is particularly evident during crises, including armed conflicts. Several factors can be distinguished to qualify them in this way. The first is its high and growing popularity. According to data as of January 2022, it is used by over 4.6 billion users worldwide,<sup>14</sup> which – at the same time – means an annual growth of 10%. The purpose of using these platforms is not only to contact friends, but also to obtain information and express one's own beliefs. However, it is not only

---

<sup>9</sup> Idem, *Władza komunikacji*, transl. J. Jedliński, P. Tomaneck, Wydawnictwo Naukowe PWN, Warszawa 2013, p. 409.

<sup>10</sup> M. Foucault, *Nadzorować i karać. Narodziny więzienia*, transl. T. Komendant, Wydawnictwo Aletheia, Warszawa 2009, p. 189.

<sup>11</sup> M. Castells, *Władza...*, p. 415.

<sup>12</sup> Idem, *Siła tożsamości*, transl. S. Szymański, Wydawnictwo Naukowe PWN, Warszawa 2009, pp. 323–331.

<sup>13</sup> *Ibidem*, p. 339.

<sup>14</sup> S. Kemp, "Digital 2022: Global Overview Report", *Data Reportal*, 26.01.2022 [on-line:] <https://datareportal.com/reports/digital-2022-global-overview-report> (23.09.2022).

the scale, but – most of all – the structure and convention of the operation of social media platforms based on the monetisation of users' attention that is the main aspect of their enormous impact.

In September 2021, the *Wall Street Journal* accessed Facebook's internal guidelines for content moderation, which it obtained from former employee Francis Haugen. These documents, submitted to the US Congress and referred to as *Facebook Papers*, indicated that the owners of the platform put their own profit much higher over security, which resulted in the admission to the public circulation of content that is controversial and arouses social unrest because it generates more traffic and user activity. Consequently, it brings more profit. It was pointed out that the loosening of moderation restrictions after the presidential elections in the US in 2020 allowed for a rapid increase in the popularity of radical groups. It could have stimulated the Capitol attack in early 2021.<sup>15</sup> The obtained information also indicates that the platform's algorithm model strengthens social polarisation by promoting emoticons expressing emotions (including anger, for example) five times more than the popular 'like'.<sup>16</sup> The lack of an appropriate number of moderators operating in different languages also means that there is a fundamental disproportion in combating disinformation content occurring in non-English-speaking countries.<sup>17</sup>

Another factor that makes social media platforms with billions of users the real subjects of power and political action is the arbitrariness and frequent lack of transparency in their decision-making. They combine, quite paradoxically, with the exclusion of social media liability for the content published by the users of their services, which is primarily guaranteed in US law, namely Section 230 *Communication Decency Act*.<sup>18</sup>

On the one hand, this means that social media platforms are not treated as media publishers, which allows them to maintain the possibility of free expression but, on the other hand, does not restrict their owners from making arbitrary decisions. Henry Kissinger stated that a laptop can make global consequences, thus referring to the

---

<sup>15</sup> C. Lima, "A Whistleblower's Power: Key Takeaways from the Facebook Papers", *Washington Post*, 26.10.2021, [on-line:] [https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/?itid=co\\_facebookunderfire\\_1](https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/?itid=co_facebookunderfire_1) (21.11.2022).

<sup>16</sup> J.B. Merrill, W. Oremus, "Five Points of Anger, One for a 'like': How Facebook's Formula Fostered Rage and Misinformation", *The Washington Post*, 26.10.2021, [on-line:] [https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/?utm\\_campaign=wp\\_main&utm\\_medium=social&utm\\_source=twitter](https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/?utm_campaign=wp_main&utm_medium=social&utm_source=twitter) (20.11.2022).

<sup>17</sup> M. Scott, "Facebook Did Little to Moderate Posts in the World's Most Violent Countries", *Politico*, 25.10.2021, [on-line:] <https://www.politico.com/news/2021/10/25/facebook-moderate-posts-violent-countries-517050>, 29 September 2022.

<sup>18</sup> *The Communication Decency Act of 1996*, 47 U.S. Code § 230.

situation where users of modern mobile phones and computers have [in their hands] an unprecedented potential for gathering, aggregating and analysing information – which was beyond the reach of many intelligence agencies in the previous generation. However, greater access to information may also be used in a direction that is undesirable from the point of view of democratic processes. Media corporations who collect a lot of detailed data about users and are able to track and even influence them, which is even beyond the capabilities of many modern countries.<sup>19</sup>

One of the co-founders of the most popular platform (Facebook) and the coordinator of Barack Obama's presidential campaign online in 2008 (Chris Hughes), in a famous column for *New York Times*, stated that the influence in the hands of Mark Zuckerberg is enormous and far beyond that of other entities in the private or public sector. The head of Facebook, operating since October 2021 as part of the Meta Group, can practically independently decide on the configuration of the platform's algorithm and, thus, determine what almost 3 billion users see and how their data is processed.<sup>20</sup> Mass spreading of false content – often as a result of specialised disinformation campaigns and monetisation of negative emotions by the platforms themselves – thus has negative consequences for democracy by strengthening epistemic cynicism (based on lowering trust in institutions and authorities), polarising discussions and give the feeling that mutual debate does not make sense due to the participation of many unidentified entities, especially bots and trolls.<sup>21</sup>

## Social media as an environment for information warfare and the creation of conflict narratives

The ongoing renewal of the war in Ukraine (since February 24, 2022) involves communication on social media platforms on an unprecedented scale. As a result, the conflict is referred to (in public discourse) as the most *viral* war or even *the first TikTok*

---

<sup>19</sup> H. Kissinger, *Porządek światowy*, transl. M. Antosiewicz, Wydawnictwo Czarne, Wołowiec 2017, p. 323.

<sup>20</sup> Ch. Hughes, "It's Time to Break Up Facebook", *New York Times*, 9.05.2019, [on-line] <https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html>, 17 September 2022.

<sup>21</sup> S. McKay, C. Tenove, "Disinformation as a Threat to Deliberative Democracy", *Political Research Quarterly*, vol. 74, no. 3 (2021), pp. 703–717.

*war* due to the high popularity of this channel in accounts of the theatre of war disseminated – particularly by civilians.<sup>22</sup>

Posting war content on social media has a variety of goals. In the case of Ukraine, these platforms are often a tool for a quick transmission of important information from the point of view of the civilian population both in Ukraine and abroad (e.g., alerts about missile attacks or information on points and the refugee aid organisation system). Above all, however, these channels allow internet users to report their wartime experiences, and viewers from almost all over the world witness them on a regular basis. In this way, expression in social media helps to maintain determination and unity in resisting, which is often reinforced with a message in the form of memes and a content based on situational comedic effect that reveal the weaknesses of the Russian army and the strength and successes of Ukraine (e.g., videos and memes about the ‘theft’ of Russian tanks by local farmers, the famous war song performed by the Ukrainian military called *Bayraktar*). The materials published on these channels are also used to build and maintain the will to help Ukraine, especially by Western states and societies. This is the aim of showing the crimes committed by Russian soldiers and shaping the narrative of the war as an existential threat to the whole of Europe, not just a local conflict.<sup>23</sup>

The very person of President Zelensky, who, in his communication on Twitter (he has 6.5 million followers), is also important for the implementation of the information policy on the part of Ukraine<sup>24</sup> because his account contains both official statements as well as non-professional video recordings that create a sense of closeness and ‘naturalness’ with the audience. The message coming from this communication is largely directed at Western countries and is aimed at influencing the provision of further assistance to Ukraine, primarily in the area of the supply of military equipment.

During the war in Ukraine, social media is also becoming a tool for disseminating opinions and sharing knowledge by analysts from the white intelligence community, the so-called “OSINT” (*open-source intelligence*) such as Belling Cat, Rochan Consulting or those who track disinformation in major Russian news channels (e.g., journalist Julia Davis, who was sanctioned by the Russian authorities for her activities).<sup>25</sup>

<sup>22</sup> M. Połowaniuk, “Rosyjska inwazja to pierwsza ‘wojna TikTokowa’”. Ukraina pokazuje, jak wygrać bitwę w sieci”, *Spider’s Web*, 28.02.2022, [on-line:] <https://spidersweb.pl/2022/02/jak-wygrac-wojne-w-internecie.html>.

<sup>23</sup> D. Ciuriak, *The Role of Social Media in Russia’s War on Ukraine*, 5.05.2022 [on-line:] [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4078863](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4078863) (28.09.2022).

<sup>24</sup> Status on 28.09.2022, [on-line:] <https://twitter.com/ZelenskyyUa>.

<sup>25</sup> Julia Davis’ Twitter account, where she publishes the results of her analysis of the narratives of major Russian news channels (entitled *Russia Media Monitor*) is followed by 353,000 users (as of September 28, 2022).

Social media platforms are also a mobilisation environment for grassroots support for Ukraine in respect of the humanitarian, military and informational dimensions. This is the dimension of the group created by internet users called NAFO (North Atlantic Fellas Organization), symbolised by the dog Shiba Inu. Its aim is to expose Russian propaganda and raise funds to support the Ukrainian army.



Figure 1. A tweet from the Ukrainian Ministry of Defence profile expressing gratitude to the NAFO movement for its activities. Source: Profile of the Ministry of Defence of Ukraine on Twitter, [online:] <https://twitter.com/defenceu/status/1563851548643426304>, (28.09.2022)

As for information warfare, social media became – especially from Russia’s point of view – an ideal tool for the implementation of disinformation campaigns, large-scale actions based on inauthentic activity and the dissemination of propaganda messages from the Russian authorities (for example, through the famous and aggressive in its message posts of the Vice-President of the Security Council of the Russian Federation, Dmitry Medvedev, on Telegram). In Russia’s confrontational actions, social media is another channel through which the fog of war can be generated, to spread panic in Western societies or reinforce uncertainty about who is guilty of committing war crimes (such as those in the maternity hospital in Mariupol or in Bucha). Reports from social media platforms regarding identified misinformative profiles and content often point

to accounts linked to Russia. Only in September 2022, Meta Concern (the owner of Facebook) announced that it had detected two extensive disinformation networks related to China and Russia. In the case of Russia, disinformation activities launched in May 2022 were based on the creation of around 60 websites imitating well-known media portals (e.g., *The Guardian*, *Bild* or *Spiegel*). The propaganda content published there was aimed at criticising Ukraine and strengthening antagonism towards refugees, building a positive Russian image and emphasising that the sanctions imposed on it are counterproductive. The content was then disseminated both organically and through purchased advertising on various social media platforms, including Facebook (with 1,633 accounts involved), Instagram, Twitter, Telegram and YouTube. This campaign, the largest since the start of the war in Ukraine, targeted audiences in Germany, Italy, the UK, France, Latvia and Ukraine. Significantly, this initially diverse audience has, over time, been limited to influencing mainly German audiences – indicating them as a key target of Kremlin propaganda.

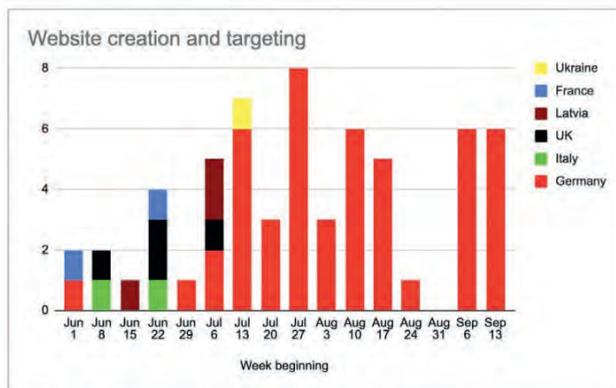


Chart 1. The number of popular media imitation sites created and their target audience. Source: B. Nimmo, M. Torrey, “Taking Down Coordinated Inauthentic Behavior from Russia and China”, Meta Detailed Report, [on-line] <https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/> (28.09.2022)

In its August 2022 report, Twitter also shared information about the identification and deletion of 38 accounts linked to pro-Kremlin media outlets. Before disseminating the Russian narrative about the war in Ukraine, their activities focused on propaganda related to the COVID-19 pandemic.<sup>26</sup>

<sup>26</sup> The analysis was based on data shared by Twitter with The Stanford Internet Observatory as part of the Moderation Research Consortium. See: *A Front for Influence: An Analysis of a Pro-Kremlin*

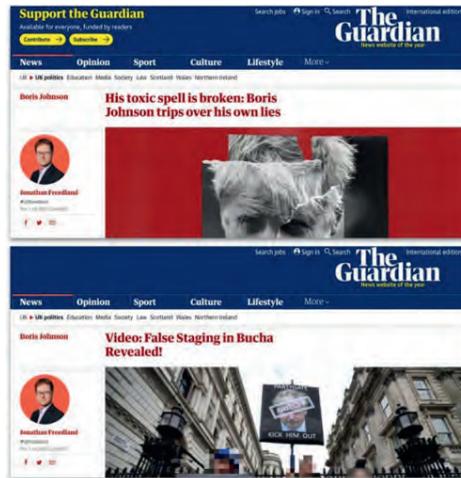


Figure 2. A screenshot from the authentic website of The Guardian – theguardian[.]com (top) versus from a website created by the Russian disinformation network to imitate this medium – theguardian[.]co[.]com (bottom) containing an article accusing Ukraine of staging the Bucha crime. Source: B. Nimmo, M. Torrey, “Taking Down Coordinated Inauthentic Behaviour from Russia and China”, Meta Detailed Report, [on-line:] <https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/> (28.09.2022)

In turn, an example of a widespread disinformation campaign, mainly in the Polish-language Twitter space, is the sudden increase in popularity of the hashtag #StopUkrainizacjiPolski, attached at the end of August 2022 to content expressing opposition to aid for refugees and generating negative attitudes towards them. The hashtag, which previously appeared on social media but never before with such popularity, was especially popular with the activists of the right-wing political party Confederation of the Polish Crown. Winning the position of hashtag leader among Polish Twitter users at the end of August this year, however, was due – as indicated by DFRLab analysis – to the artificial manipulation of traffic generated by a group of hyperactive accounts (according to this analysis, ten accounts accounted for as much as 16% of all, approximately 46,000 hashtag-related activities undertaken between 24–27 August 2022).<sup>27</sup> An analysis of the further popularity of the hashtag made by the author of the article shows that on September 10–17, activity related to it decreased

*Network Promoting Narratives on COVID-19 and Ukraine* [on-line:] <https://cyber.fsi.stanford.edu/io/news/sio-aug-22-takedowns-ua> (28.09.2022).

<sup>27</sup> G. Gigitashvili, *Twitter Campaign Pushes Anti-Ukraine Hashtag into Poland’s Trending List*, 8.2022 [on-line:] <https://medium.com/dfrlab/twitter-campaign-pushes-anti-ukraine-hashtag-into-polands-trending-list-90ccc9474a60> (22.11.2022).

(a total of 5,857 activities were recorded, including 743 tweets, 3,388 retweets and 1,726 replies). However, it was noted that more than 30% of the tweets came from two profiles whose activity clearly increased during the peak of the hashtag's popularity. At the same time, it was shown that both of these accounts were publishing about 30 tweets a day, which suggests suspicions of inauthentic or propaganda-oriented activity.<sup>28</sup>

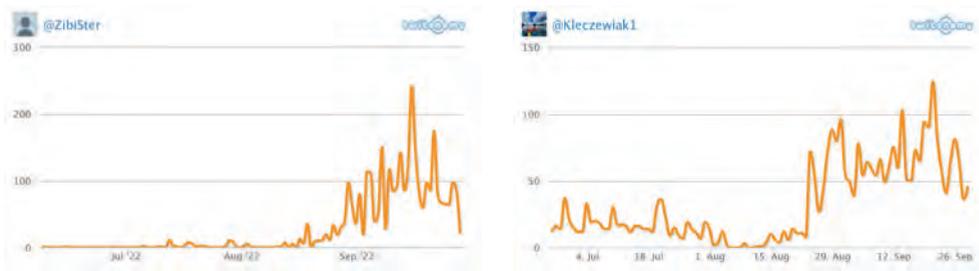


Chart 2. Three-month activity (tweets, retweets and replies) of two accounts publishing the most tweets with the hashtag #StopUkrainalizacjiPolski on 10-17.09.2022. Source: own analysis using the Twitonomy tool

## Social media as an object of political activities, especially in the fight against disinformation

Numerous disinformation campaigns, as well as the Cambridge Analytica case (when data from 87 million Facebook user accounts were used for political micro-targeting) were important triggers for various actors to combat this practice, including increasing the accountability of social media platforms for their content.<sup>29</sup> They included both legislative solutions (e.g., laws adopted in France, Germany or Austria) as well as activities related to the early detection of disinformation campaigns and increasing social resistance to their impact. The large-scale fight against *fake news* contributed to the emergence of specialised entities such as the Centre Against Terrorism and Hybrid Threats (CTHH) in the Czech Republic or the European Centre of Excellence for Countering Hybrid Threats established in April 2017 (*Hybrid CoE*), an embodiment

<sup>28</sup> Data on number of tweets was obtained from the Twitter API via the MAXQDA software. The analysis of the activity of individual profiles was carried out using the Twitonomy tool.

<sup>29</sup> F. Saurwein, C. Spencer-Smith, "Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe", *Digital Journalism*, vol. 8, no 6 (2020), pp. 820-841.

of the interaction between the EU and NATO.<sup>30</sup> Furthermore, the EU, in March 2015, had already taken steps to combat Russian disinformation, particularly in the Eastern Partnership countries, by establishing a task force within the framework of the European External Action Service (EEAS) *East Strat Com*. Its flagship project is *EUvsDisinfo*, aimed at monitoring the pro-Kremlin media and the propaganda they spread, which is currently of particular importance during the ongoing war in Ukraine and intensified disinformation activities at that time.<sup>31</sup> It is also worth to mention, an important role of non-governmental organisations in countering disinformation. In this regard this role is played especially by the international community of fact-checking organisations, *International Fact-Checking Network*, which consists of around 100 entities to verify the content on online platforms.

An important aspect of the actions taken in the fight against disinformation was the attempt to find a balance between two key values, namely freedom of expression and ensuring security. While the sphere of combating disinformation by detecting and giving an early warning [to the public] of false narratives does not enter into this dilemma so much, actions taken in the legislative arena are often met with concerns about restrictions on freedom of speech. The lack of a strictly defined meaning of the terms such as disinformation or *fake news* both in the media and scientific discourse<sup>32</sup> are often used – in particular, under authoritarian regimes to limit the freedom of citizens. This is the case, for example, in Russia, where since 2019, dissemination of false information that may harm life and health, public order and safety, as well as content that expresses disrespect for the authorities and state symbols of the Russian Federation is penalised with a fine or 15-day detention.<sup>33</sup>

Dilemmas over the scope of the solutions introduced in this regard are also present in democratic states, which have introduced new obligations on social media platforms to combat disinformation or hate speech in their legislation. This was the case, for example, in Germany, where the regulations of the *Network Enforcement Act*

---

<sup>30</sup> M. Danek, “Modele walki z dezinformacją: od restrykcji do współpracy”, in M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds), *Znaczenie nowych technologii dla jakości systemu politycznego. Ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020, p. 138.

<sup>31</sup> The project’s website contains both research and reports presenting the results of conducted monitoring, as well as a database allowing users to search for individual media content on their own. See Project website [on-line:] <https://euvsdisinfo.eu/pl/#> (28.09.2022).

<sup>32</sup> E.C. Tandoc Jr., Z.W. Lim, R. Ling, “Defining ‘Fake News’: A Typology of Scholarly Definitions”, *Digital Journalism*, vol. 6, no. 2 (2018), pp. 137–153.

<sup>33</sup> “Russia Passes Legislation Banning ‘Disrespect’ of Authorities and ‘Fake News’”, *The Moscow Times*, 7.03.2019 [on-line:] <https://www.themoscowtimes.com/2019/03/07/russia-passes-legislation-banning-disrespect-of-authorities-and-fake-news-a64742> (29.09.2022).

(NetZDG), in force since 2018, were met with criticism from the opposition.<sup>34</sup> *The Online Safety Bill*, currently under consideration in the UK, is also controversial due to the requirement for social media platforms to tackle not only illegal content, but also content that is described as legal but harmful, which has led to fears of censorship.<sup>35</sup>

The war in Ukraine emphasised this dilemma even more. The extraordinary circumstances related to the security crisis created expectations to cross the existing borders in the context of increasing security and ensuring freedom of expression. There has been an expectation and even a pressure towards social media platforms on the part of Western countries – as well as Ukraine – to act not so much as a neutral actor, but as an active influence entity in the fight against Russian propaganda. Responding to these expectations, both Meta and Twitter started, from the beginning of the conflict, to specifically flag and restrict the visibility of content from Russian media. Then, following the introduction of EU-level sanctions, they blocked the accounts of two key Kremlin tubes (Sputnik and Russia Today).<sup>36</sup> In response to the actions taken by the platforms, Facebook, Instagram and Twitter were blocked in Russia by the decision of *Roskomnadzor*.<sup>37</sup>

In turn, Ukrainian political actors emphasise that these platforms must give up their position of technical neutrality in favour of becoming allies in shaping the information environment of the ongoing war. In this approach, more emphasis is placed on freedom of speech, especially in terms of reporting on Russian war crimes. As President Zelenskiy noted in one of his tweets, “War is not only a military opposition on UA land. It is also a fierce battle in the informational space.”<sup>38</sup> The politician then expressed his gratitude to Meta and other social media platforms for their solidarity with Ukraine in this field. However, one can notice that content reporting on events in Ukraine is often blocked due to automated algorithms or the activity of Russian-

<sup>34</sup> M. Danek, “Komunikowanie polityczne w dobie fake newsów – walka z dezinformacją w sieci”, *Krakowskie Studia Małopolskie*, vol. 23 (2018), pp. 210–228.

<sup>35</sup> “Online Safety Bill to Return as Soon as Possible”, *BBC*, 20.09.2022, [on-line:] <https://www.bbc.com/news/technology-62908598> (29.09.2022).

<sup>36</sup> “Kalendarium – sankcje UE wobec Rosji w sprawie Ukrainy”, *Strona Rady Europejskiej i Rady Unii Europejskiej*, [on-line:] <https://www.consilium.europa.eu/pl/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/> (29.09.2022).

<sup>37</sup> “Facebook i Twitter zablokowane w Rosji”, *Wirtualne Media*, 5.03.2022, [on-line:] <https://www.wirtualnemedi.pl/artykul/rosja-blokada-facebook-twitter> (29.09.2022).

<sup>38</sup> Quoted from: Volodymyr Zelenskiy’s tweet of March 13, 2022, [on-line] [https://twitter.com/ZelenskyyUa/status/1503046528071618562?ref\\_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1503046528071618562%7Ctwgr%5E69f0efacb3b90149cdb32cd47fa434406cf5c877%7Ctwcon%5Es1\\_&ref\\_url=https%3A%2F%2Fdorzeczy.pl%2Fopinie%2F275323%2Fzelenski-dziekuje-mecie-wojna-to-nie-tylko-konfrontacja-militarna.html](https://twitter.com/ZelenskyyUa/status/1503046528071618562?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1503046528071618562%7Ctwgr%5E69f0efacb3b90149cdb32cd47fa434406cf5c877%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fdorzeczy.pl%2Fopinie%2F275323%2Fzelenski-dziekuje-mecie-wojna-to-nie-tylko-konfrontacja-militarna.html) (29.09.2022).

linked accounts that report it as material that does not comply with the platforms' terms of service. This was pointed out by Mykhailo Fedorov, Deputy Prime Minister and Minister of Digital Transformation of Ukraine, who – in a July 2022 letter to Nick Clegg, CEO of Global Policy Meta Corporation, on the moderation of Ukrainian content – stressed that the truth about the Russian invasion could not resonate enough when social media policy is created *only for the time of peace*.<sup>39</sup> He also pointed out the need to provide the Ukrainian side with a so-called “market-specific slur lists” (i.e., an internal and periodically updated document by Meta to help moderators adjudicate violations of the rules of procedure in relation to the cultural context).<sup>40</sup> According to Fedorov, this will allow to limit the cases of excessive and incorrect imposition of restrictions on content.

Finally, it should be noted that during the ongoing armed conflict, the fight against disinformation entered the next level in the context of EU actions. It is the result of a policy that has been in place for several years in this area, and was intensified – in particular – before the European Parliament elections in 2019. The previously adopted acts, especially in the form of self-regulation of digital platforms, such as the Code of Practice on Disinformation,<sup>41</sup> were supplemented by the Digital Service Act (DSA)<sup>42</sup> and Digital Market Act (DMA) regulations adopted in 2022, regulating the digital platform market. The EU's work also resulted in a clear definition of disinformation, which excluded satire, parody, reporting errors or biased opinions.<sup>43</sup>

---

<sup>39</sup> “Мінцифра звернулася з листом до Meta щодо модерації українського контенту”, *The Digital*, [on-line:] <https://thedigital.gov.ua/news/mintsifra-zvernulasya-z-listom-do-meta-shchodomodratsii-ukrainskogo-kontentu> (29.09.2022).

<sup>40</sup> “Jak tworzymy i wykorzystujemy listy zniewag typowych dla danego rynku”, *Transparency Center*, 12.08.2022, [on-line:] <https://transparency.fb.com/pl-pl/enforcement/taking-action/how-we-create-and-use-market-slurs> (29.09.2022).

<sup>41</sup> The first version of the Code was implemented in 2018, and after periodic evaluation, it was decided to strengthen and specify its provisions. It obliges its signatories, i.a. Meta, Google, Twitter, TikTok and Microsoft to increase the transparency of their activities, demonetize disinformation, identify fake accounts increase, transparency of political advertisements, cooperate with fact-checking organizations and the scientific community. Currently, 34 entities are signatories to it, and in addition to digital platforms, it has also been joined by non-governmental organizations dealing with the fight against disinformation. See: *2022 Strengthened Code of Practice on Disinformation*, 16.06.2022, [on-line:] <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation> (29.09.2022).

<sup>42</sup> COM(2020) 825 final, *Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE*, 15.12.2020 [on-line:] <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020PC0825> (29.09.2022).

<sup>43</sup> Disinformation was defined as *verifiably false or misleading information created, presented and disseminated for the purpose of obtaining economic advantage or misleading the public, which is likely to cause public harm*. Public harm, in turn, was linked to threats to democratic political processes

Thanks to the actions taken, social media platforms have been obliged to increase the transparency of their activities by publishing periodic reports on the rules and effects of content moderation or the number and type of requests for access to user data submitted by state authorities.<sup>44</sup> The platforms were also obliged to create ads libraries which allow, in particular in the aspect of political messages, them to be analysed in terms of sponsors, financial resources and targeting criteria (although they are presented only concerning a few main variables, such as place of residence or sex).<sup>45</sup>

At the same time, it should be noted that social media platforms have started cooperation with third parties (scientists, journalists, NGOs, etc.) in content moderation. This has taken on a rather formalised form in the case of Meta, which has set up a so-called “Oversight Board”, composed partly of members designated by the company itself and partly by representatives from the expert community, especially academia. The board investigates complaints from Facebook and Instagram users<sup>46</sup> on decisions made by platforms moderators, as well as taking actions on its own behalf on the basis of content monitoring. Meta can also turn to the council to take a position on a given matter.<sup>47</sup> The effects of the work of this body are binding decisions regarding the removal or restoration of previously deleted content, as well as non-obligatory recommendations related to the improvement of Meta’s terms of service in the field of content moderation. Among the issues raised and considered by the board was the

---

and the formation of policy and to public goods. See: COM(2018) 236 final, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Zwalczenie dezinformacji w Internecie: podejście europejskie*, 26.04.2020, [on-line:] <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52018DC0236> (29.09.2022).

<sup>44</sup> *Meta Transparency Center*, [on-line:] <https://transparency.fb.com/pl-pl/>; *Twitter Transparency Center*, [on-line:] <https://transparency.twitter.com/> (29.09.2022).

<sup>45</sup> See: *Meta Ads Library*, [on-line:] [https://www.facebook.com/ads/library/?active\\_status=all&ad\\_type=political\\_and\\_issue\\_ads&country=PL&media\\_type=all](https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=PL&media_type=all) (29.09.2022). Twitter owners do not maintain an up-to-date Ad Library, as they decided in 2019 to remove politics-related advertising, arguing that political coverage should be gained, not bought. See: “Twitter będzie blokował reklamy polityczne. Dorsey kpi ze stanowiska Facebooka”, *Wirtualne Media* [on-line:] <https://www.wirtualnemedial.pl/artykul/twitter-bedzie-blokowal-reklamy-polityczne-dorsey-kpi-ze-stanowiska-facebook> (29.09.2022).

<sup>46</sup> A request to the Board for a case to be considered can only be made after exhausting the appeal path within the platform’s internal procedure.

<sup>47</sup> It is worth adding that the Board does not issue decisions on all reported cases, but only on those it deems the most controversial and key in the selection process. In practice, this number is very low compared to the reported complaints. According to the report for the first quarter of 2022, out of over 479 thousand, only three of the reported cases were selected for consideration, two of which were reported by users and one by Meta. See: “Oversight Board Q1 2022 Transparency Report”, *Oversight Board*, 8.2022, [on-line:] <https://oversightboard.com/news/572895201133203-oversight-board-publishes-transparency-report-for-first-quarter-of-2022/> (29.09.2022).

decision to reinstate a comment under a post reporting on the protests in Russia in support of Alexei Navalny, under which its author called a user who criticised their participants (claiming that shamelessly abused and mentally retarded people took part) *a cowardly bot*. The board considered that while the deletion of the comment may have been in line with community standards, this failed to take into account the wider political context, disproportionately restricting freedom of expression.<sup>48</sup> This position shows that the rigid application of platform regulations can be disadvantageous, especially in countries where the authorities restrict freedom of speech.

Such situations can be mitigated by the aforementioned DSA, which introduces several significant changes in the context of reducing the social impact of disinformation. These include, in particular, limiting the use of sensitive data (e.g., on political views or religion), clarifying the logic behind the algorithms or making content moderation more transparent. Users are to receive a detailed explanation of the reasons for removing or limiting the visibility of their content, and above all it's a human, not an algorithm, who must examine appeals against this decision. In addition, new EU law categorises service providers according to their social impact, identifying the major online platforms (with at least 10% of the EU population, i.e., at least 45 million users today) with the greatest obligations. In addition to upholding the order associated with the ads libraries, they must ensure an adequate level of moderation in all EU languages by hiring additional moderators, performing a periodic risk analysis of their activities or providing an alternative system for selecting content recommendations to that suggested by the algorithm.<sup>49</sup>

In addition, under the regulation, digital service coordinators will be appointed in each EU Member State. Their role will be related not only to monitoring the implementation of DSA regulations, but also to handling user complaints regarding the infringement of their rights. The changes introduced in DSA (in the context of security crises) are, therefore, important in terms of increasing the transparency of the operation of social media platforms and the principles of targeting political advertising – which may affect more effective monitoring of their activities (also in cooperation with the scientific community) and earlier response to possible risks. More transparent moderation rules have the potential to reduce the arbitrariness of social media platforms

---

<sup>48</sup> “Pro-Navalny protests in Russia”, *Oversight Board*, [on-line:] <https://www.oversightboard.com/decision/FB-6YHRXHZR/> (29.09.2022).

<sup>49</sup> In July 2022, Meta launched a new news feed system on Facebook called *Home*, which allows users to independently decide on the order of displayed content. See: “Introducing Home and Feeds on Facebook”, *Meta*, [on-line] <https://about.fb.com/news/2022/07/home-and-feeds-on-facebook/> (29.09.2022).

in deciding the visibility of content, and the introduction of an alternative form of *news feed* may also<sup>50</sup> contribute to reducing the so-called “filter bubble mechanism” (i.e., a situation where social media users function in a closed environment of uniform and often controversial and manipulated opinions). However, this does not change the fact that the individual provisions contained in the DSA are often formulated at a high level of generality, and the shape of their implementation depends on the social media platforms themselves (e.g., the rule that online platforms suspend for a reasonable period the provision of services to audiences that frequently transmit illegal content).<sup>51</sup> Therefore, it is necessary to constantly monitor the implementation of the content of the regulation – both in the context of the transparency of the activity of the platforms and the question of their actions towards restriction of freedom of expression as well as the whole contribution to reducing the negative impact of manipulative content. National digital service coordinators and the trusted entities appointed and cooperating with them, based on the provisions of the DSA, will play a significant role in this respect.

## Social media platforms as decision-making entities in the context of the war in Ukraine

The extraordinary circumstances of the security crisis triggered by Russia’s aggression against Ukraine also provoked actions by the social media platforms managers, which were taken on their own initiative as actors of influence on political realities. On the one hand, they are an expression of the continuation of their previous policy, mainly in terms of increasing the effectiveness of content moderation but on the other one can notice the introduction of new initiatives that go beyond the applicable regulations. Both Meta and Twitter have published [on their sites] lists of actions they have taken to minimise the negative effects of war-related disinformation, as well as to help the civilian population<sup>52</sup> – which is also important for building a positive image [of the platforms].

---

<sup>50</sup> It is worth noting that the algorithm will remain the default option. Thus, users themselves will have to decide whether they want to use a different option for selecting content.

<sup>51</sup> COM(2020) 825 final, *Rozporządzenie*.

<sup>52</sup> Information on the actions taken by Meta and Twitter comes from the companies’ websites devoted to the subject, unless another source is mentioned in a footnote. See: S. McSweeney, “Our Ongoing Approach to the War in Ukraine”, *Twitter*, [on-line:] [https://blog.twitter.com/en\\_us/topics/company/2022/our-ongoing-approach-to-the-war-in-ukraine](https://blog.twitter.com/en_us/topics/company/2022/our-ongoing-approach-to-the-war-in-ukraine) (29.09.2022); “Meta’s Ongoing

Meta has established a special information centre with moderators who are fluent in Ukrainian and Russian to monitor the content on the platforms continuously. In addition, the concern has increased the protection of the privacy of users from Ukraine by introducing, among others, simple functionality of blocking a profile or preventing third parties from viewing their list of friends. A dedicated *Community Help* sphere has also been set up on Facebook, especially for refugees from Ukraine, where information is shared (e.g., from UN agencies) on the availability of medical assistance in Ukraine and bordering countries. It is complemented by a hotline created by the Ukrainian state services on WhatsApp messenger, where key information related to crisis management is published on an ongoing basis. In addition, Meta, within the scope of its *Data for Good* project, shares information on users' social connectedness and mobility with various trusted entities (e.g., the World Bank, Doctors Without Borders), which helps to track the flow of refugees, for example.

Both Meta and Twitter have highlighted the importance of providing higher-quality content moderation. Even before the aforementioned blocking of the accounts of major Russian media outlets, the companies had already decided to reduce the visibility of the content they disseminate, demonetise their activities and clearly mark that they are linked to Russia. Additionally, Twitter blocked the possibility of buying ads in Russia and Ukraine, and in connection with content related to the subject of the war. In addition, the platform has introduced a rule that it will not recommend users content published by representatives of governments of countries that restrict free access to information and are involved in armed conflicts. This rule was primarily applied to Russia. Twitter also introduced changes to the system of recommending content to users from Russia and Ukraine, excluding tweets from entities that they do not currently follow. In addition, based on its internal assessments, the platform reduces the visibility of content that does not explicitly violate the platform's regulations, but may contribute to social harm. Meta was more arbitrary and decided to temporarily suspend its rules of procedure concerning hate speech and allow Ukrainian users to express it in relation to the Russian aggressors. Initial reports by Reuters in early March, based on information from internal company emails, indicated that Facebook and Instagram users from Ukraine and several countries (Armenia, Azerbaijan, Georgia, Hungary, Poland, Romania, Russia, Slovakia and the Baltic States) would be able to call for the death of soldiers – and even political leaders – led by Vladimir Putin. A few days later, the representative of Meta, Nick Clegg, stipulated that this time-limited

---

Efforts Regarding Russia's Invasion of Ukraine", *Meta*, 26.20.2022, [on-line:] <https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/#latest> (29.09.2022).

change in the company's moderation policy would only apply to Ukraine and would allow its citizens to "express their resistance and fury at the invading military forces, which would rightly be viewed as unacceptable", while pointing out that hate speech against Russians would still be banned. In conclusion it can be stated that the social media platform made an arbitrary decision that goes beyond the regulations in the face of extraordinary circumstances. In response to these reports, Russia recognised Facebook and Instagram as extremist entities and blocked their operation in Russia. This sanction is a kind of determinant of the position of the largest social media platforms in the context of their impact on shaping the information space, which, as previously indicated, is one of the crucial fields of power and political relations in their confrontational dimension.

## Summary

The conducted analysis allows to conclude that social media platforms are not neutral technical tools for disseminating content on a mass scale, but a means of exerting influence, particularly through disinformation and propaganda. This makes them a key information battlefield, especially in security crises taking the form of hybrid wars. Moreover, the owners of these platforms themselves can be described as sensitive actors of influence and power. Unlike traditional political actors (states, international organisations), they use this power and influence in the form of arbitrary and not always transparent procedures. The security crisis triggered by the war has also shown that political actors often expect social media platforms to abandon neutrality in favour of a commitment to defend higher values.

Nevertheless, social media play an important role in shaping the narrative towards the conflict, which was skilfully used primarily by Ukraine. They can be seen also as the channels of mass dissemination of information that may be of importance for crisis management activities. With regard to the spread of disinformation, it seems that actions taken by many actors, including social media platforms themselves, to limit it are needed. However, they will not completely eliminate the spread of manipulated content on a large scale as they must always balance between key values of freedom of expression and security. An experiment carried out by the NATO Strategic Communication Centre of Excellence (NATO StratCom Coe) between September and November 2021<sup>53</sup> involving the purchase of more than 114,000 inauthentic activities

---

<sup>53</sup> NATO StratCom Coe, "Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation", *NATO Strategic Communications Centre of*

(posts, comments, views) on Facebook, Instagram, YouTube, Twitter, Tiktok and VKontakte platforms for €279, based on Russian social media manipulation strategies, showed that 96% of them still remained active after a four-week period. This is sufficient time to spread disinformation to even millions of users, and any remedial action taken after that time may be delayed. This study indicates that the internal mechanism of platforms in combating disinformation campaigns is unreliable, the more so that the disinformation activity initiated by bots or trolls is then reinforced and sustained by the users themselves, who also become *curators* of these narratives.<sup>54</sup> The problem will continue to worsen, not only due to the aggressive actions in the information space undertaken by Russia or China, but the fact that younger generations, compared to older ones, rely much more on social media as sources of information about the world. From a Polish point of view, this is all the more important because, as Eurobarometer surveys have shown, Poles are the most uncertain of all EU nations as to whether they can recognise disinformation (40% of indications against an EU average of 30%).<sup>55</sup>

In the *National Security Strategy of the Republic of Poland*, in the aspect of information space management, an emphasis was placed on counteracting disinformation, building short-term and long-term communication strategies in cyberspace, cooperating with mass media, social media and non-governmental organisations, as well as building social resistance to campaigns of manipulated content. This approach seems to cover all the key elements of managing the new media environment, including educating citizens to operate in it safely and responsibly.<sup>56</sup>

The experience of the war in Ukraine has underlined the critical role of the social education in respect of methods of recognising and dealing with disinformation. It is a premise, that the social media platforms will be used more responsibly (e.g., by choosing an alternative method of displaying content to the algorithm). The decision to contextualise content moderation made by the owners of Meta in response to the war in Ukraine may be perceived, on the one hand, as taking the right side of

---

*Excellence*, 27.04.2022, [on-line:] <https://stratcomcoe.org/publications/social-media-manipulation-20212022-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/242> (29.09.2022).

<sup>54</sup> Y. Golovchenko, M. Hartmann, R. Adler-Nissen, "State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation", *International Affairs*, vol. 94, no. 5 (2018), pp. 975–994.

<sup>55</sup> Survey conducted at the turn of April and May 2022, See: Flash Eurobarometr, *News&Media Survey*, [on-line] <https://europa.eu/eurobarometer/surveys/detail/2832> (29.09.2022).

<sup>56</sup> *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, Warszawa 2020, [on-line] [https://www.bbn.gov.pl/ftp/dokumenty/Strategia\\_Bezpieczenstwa\\_Narodowego\\_RP\\_2020.pdf](https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf) (28.09.2022).

the conflict, but on the other, it also reveals a dangerous tendency to arbitrarily make decisions that have a key impact on shaping the public debate and thus the exercise of power in a networked society. Therefore, it is important for the state administration as well as NGOs to actively cooperate and monitor the activity of the social media platforms, which, among others, is expressed in the provisions of the DSA, so that a wider group of actors takes key decisions for shaping the narrative. However, the most important action should be to make citizens aware that in the era of a highly individualised media environment, they also have greater responsibility in searching for reliable sources of information and functioning in the space of many, sometimes controversial opinions.<sup>57</sup> Such an approach will help both reduce the negative impact of social media platforms on democratic debate and, at the same time, protect the digital space from attempts to arbitrarily restrict it in terms of freedom of speech in favour of superior and broadly understood security.

## References

- 2022 *Strengthened Code of Practice on Disinformation*, 16.06.2022, [on-line:] <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>.
- Bastos M.T., Mercea D., “The Brexit Botnet and User-generated Hyperpartisan News”, *Social Science Computer Review*, vol. 37, no. 1 (2019), pp. 38–54, <https://doi.org/10.1177/0894439317734157>.
- Bilal A., “Hybrid Warfare – New Threats, Complexity, and ‘Trust’ as the Antidote”, *NATO Review* 2021, [on-line:] <https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html>.
- Castells M., *Siła tożsamości*, transl. S. Szymański, Wydawnictwo Naukowe PWN, Warszawa 2009.
- Castells M., *Spółeczeństwo sieci*, crowd. M. Marody et al., transl. M. Marody, Wydawnictwo Naukowe PWN, Warszawa 2011.
- Castells M., *Władza komunikacji*, transl. J. Jedliński, P. Tomanek, Wydawnictwo Naukowe PWN, Warszawa 2013.
- Ciuriak D., *The Role of Social Media in Russia’s War on Ukraine*, 5.05.2022, [on-line:] [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=4078863](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4078863).
- COM(2020) 825 final, *Rozporządzenie Parlamentu Europejskiego i Rady w sprawie jednolitego rynku usług cyfrowych (akt o usługach cyfrowych) i zmieniające dyrektywę 2000/31/WE*, 15.12.2020, [on-line:] <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52020PC0825>.

<sup>57</sup> A. Jungherr, R. Schroeder, “Disinformation and the Structural Transformations of the Public Arena: Addressing the Actual Challenges to Democracy”, *Social Media+Society*, vol. 7, no. 1 (2021), pp. 1–13.

- COM(2018) 236 final, *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Zwalczenie dezinformacji w Internecie: podejście europejskie*, 26.04.2020, [on-line:] <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52018DC0236>.
- The Communication Decency Act of 1996*, 47 U.S. Code § 230.
- Danek M., “Komunikowanie polityczne w dobie fake newsów – walka z dezinformacją w sieci”, *Krakowskie Studia Małopolskie*, vol. 23 (2018), pp. 210–228, <https://doi.org/10.15804/ksm201811>.
- Danek M., “Modele walki z dezinformacją: od restrykcji do współpracy”, in M. Bernaczyk, T. Gąsior, J. Misiuna, M. Serowaniec (eds), *Znaczenie nowych technologii dla jakości systemu politycznego. Ujęcie politologiczne, prawne i socjologiczne*, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2020.
- Dijk van J., *Społeczne aspekty nowych mediów*, transl. J. Konieczny, Wydawnictwo Naukowe PWN, Warszawa 2010.
- EUvsDisinfo*, [on-line:] <https://euvsdisinfo.eu/pl/#>.
- “Facebook i Twitter zablokowane w Rosji”, *Wirtualne Media*, 5.03.2022, [on-line:] <https://www.wirtualnemedi.pl/artykul/rosja-blokada-facebook-twitter>.
- Flash Eurobarometr, *News&Media Survey*, 6.2022, [on-line:] <https://europa.eu/eurobarometer/surveys/detail/2832%20>.
- Foucault M., *Nadzorować i karać. Narodziny więzienia*, transl. T. Komendant, Wydawnictwo Aletheia, Warszawa 2009.
- A Front for Influence: An Analysis of a Pro-Kremlin Network Promoting Narratives on COVID-19 and Ukraine*, 24.08.2022, [on-line] <https://cyber.fsi.stanford.edu/io/news/sio-aug-22-takedowns-ua>.
- Gerasimow V., “The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations”, *Military Review* (2016), pp. 23–29, [https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview\\_20160228\\_art008.pdf](https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf).
- Gigitashvili G., *Twitter Campaign Pushes Anti-Ukraine Hashtag into Poland's Trending List*, 8.2022, [on-line:] <https://medium.com/dfrlab/twitter-campaign-pushes-anti-ukraine-hashtag-into-polands-trending-list-90ccc9474a60>.
- Golovchenko Y., Hartmann M., Adler-Nissen R., “State, Media and Civil Society in the Information Warfare over Ukraine: Citizen Curators of Digital Disinformation”, *International Affairs*, vol. 94, no. 5 (2018), pp. 975–994, <https://doi.org/10.1093/ia/iiy148>.
- Guess A., Nyhan B., Reifler J., *Selective Exposure to Misinformation: Evidence from the Consumption of Fake News during the 2016 US Presidential Campaign*, 9.01.2018, [on-line:] <https://about.fb.com/wp-content/uploads/2018/01/fake-news-2016.pdf>.
- Hughes Ch., “It’s Time to Break Up Facebook”, *The New York Times*, 9.05.2019, [on-line:] <https://www.nytimes.com/2019/05/09/opinion/sunday/chris-hughes-facebook-zuckerberg.html>.
- “Introducing Home and Feeds on Facebook”, *Meta*, 21.07.2022, [on-line:] <https://about.fb.com/news/2022/07/home-and-feeds-on-facebook/>.

- “Jak tworzymy i wykorzystujemy listy zniewag typowych dla danego rynku”, *Transparency Center*, 12.08.2022, [on-line:] <https://transparency.fb.com/pl-pl/enforcement/taking-action/how-we-create-and-use-market-slurs>.
- Jungherr A., Schroeder R., “Disinformation and the Structural Transformations of the Public Arena: Addressing the Actual Challenges to Democracy”, *Social Media+Society*, vol. 7, no. 1 (2021), <https://doi.org/10.1177/2056305121988928>.
- “Kalendarium – sankcje UE wobec Rosji w sprawie Ukrainy”, *Strona Rady Europejskiej i Rady Unii Europejskiej*, [on-line:] <https://www.consilium.europa.eu/pl/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/>.
- Kemp S., “Digital 2022: Global Overview Report”, *DataReportal*, 26.01.2022, [on-line:] <https://datareportal.com/reports/digital-2022-global-overview-report>.
- Kissinger H., *Porządek światowy*, transl. M. Antosiewicz, Wydawnictwo Czarne, Wołowiec 2017.
- Lima C., “A Whistleblower’s Power: Key Takeaways from the Facebook Papers”, *Washington Post*, 26.10.2021, [on-line:] [https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/?itid=co\\_facebookunderfire\\_1](https://www.washingtonpost.com/technology/2021/10/25/what-are-the-facebook-papers/?itid=co_facebookunderfire_1).
- McKay S., Tenove C., “Disinformation as a Threat to Deliberative Democracy”, *Political Research Quarterly*, vol. 74, no. 3 (2021), <https://doi.org/10.1177/1065912920938143>.
- McSweeney S., “Our Ongoing Approach to the War in Ukraine”, *Twitter*, [on-line:] [https://blog.twitter.com/en\\_us/topics/company/2022/our-ongoing-approach-to-the-war-in-ukraine](https://blog.twitter.com/en_us/topics/company/2022/our-ongoing-approach-to-the-war-in-ukraine).
- Merrill J.B., Oremus W., “Five Points of Anger, One for a ‘Like’: How Facebook’s Formula Fostered Rage and Misinformation”, *The Washington Post*, 26.10.2021, [on-line:] [https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/?utm\\_campaign=wp\\_main&utm\\_medium=social&utm\\_source=twitter](https://www.washingtonpost.com/technology/2021/10/26/facebook-angry-emoji-algorithm/?utm_campaign=wp_main&utm_medium=social&utm_source=twitter).
- Meta Ads Library*, [on-line:] [https://www.facebook.com/ads/library/?active\\_status=all&ad\\_type=political\\_and\\_issue\\_ads&country=PL&media\\_type=all](https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=PL&media_type=all).
- “Meta’s Ongoing Efforts Regarding Russia’s Invasion of Ukraine”, *Meta*, 26.20.2022, [on-line:] <https://about.fb.com/news/2022/02/metas-ongoing-efforts-regarding-russias-invasion-of-ukraine/#latest>.
- Meta Transparency Center*, [on-line:] <https://transparency.fb.com/pl-pl/>.
- “Mincifra zvernułasâ z listom do Meta šodo moderacii ukrâins’kogo kontentu” [“Мінцифра звернулася з листом до Meta щодо модерації українського контенту”], *The Digital*, 27.07.2022, [on-line:] <https://thedigital.gov.ua/news/mintsifra-zvernułasya-z-listom-do-meta-shchodo-moderatsii-ukrainskogo-kontentu>.
- NATO StratCom Coe, “Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation”, *NATO Strategic Communications Centre of Excellence*, 27.04.2022, [on-line:] <https://stratcomcoe.org/publications/social-media-manipulation-20212022-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/242>.
- “Online Safety Bill to Return as Soon as Possible”, *BBC*, 20.09.2022, [on-line:] <https://www.bbc.com/news/technology-62908598>.

- “Oversight Board Q1 2022 Transparency Report”, *Oversight Board*, 8.2022, [on-line:] <https://oversightboard.com/news/572895201133203-oversight-board-publishes-transparency-report-for-first-quarter-of-2022/>.
- Połowaniuk M., “Rosyjska inwazja to pierwsza ‘wojna TikTokowa’ Ukraina pokazuje, jak wygrać bitwę w sieci”, *Spider’s Web*, 28.02.2022, [on-line:] <https://spidersweb.pl/2022/02/jak-wygrac-wojne-w-internecie.html>.
- Profile of Volodymyr Zelensky on Twitter, [on-line:] <https://twitter.com/ZelenskyyUa>.
- “Pro-Navalny Protests in Russia”, Oversight Board, [on-line:] <https://www.oversightboard.com/decision/FB-6YHRXHZR/>.
- Putnam R., *Samotna gra w kręgle. Upadek i odrodzenie wspólnot lokalnych w Stanach Zjednoczonych*, transl. P. Sadura, S. Szymański, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008.
- Rocha Y.M. et al., “The Impact of Fake News on Social Media and Its Influence on Health during the COVID-19 Pandemic: A Systematic Review”, *Journal of Public Health* (2021), <https://doi.org/10.1007/s10389-021-01658-z>.
- “Russia Passes Legislation Banning ‘Disrespect’ of Authorities and ‘Fake News’”, *The Moscow Times*, 7.03.2019, [on-line:] <https://www.themoscowtimes.com/2019/03/07/russia-passes-legislation-banning-disrespect-of-authorities-and-fake-news-a64742>.
- Saurwein F., Spencer-Smith C., “Combating Disinformation on Social Media: Multilevel Governance and Distributed Accountability in Europe”, *Digital Journalism*, vol. 8 no. 6 (2020), pp. 820–841, <https://doi.org/10.1080/21670811.2020.1765401>.
- Scott M., “Facebook Did Little to Moderate Posts in the World’s Most Violent Countries”, *Politico*, 25.10.2021, [on-line:] <https://www.politico.com/news/2021/10/25/facebook-moderate-posts-violent-countries-517050>.
- “Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020”, GOV, Warszawa 2020, [on-line:] [https://www.bbn.gov.pl/ftp/dokumenty/Strategia\\_Bezpieczenstwa\\_Narodowego\\_RP\\_2020.pdf](https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf).
- Sun Tzu, *Sztuka wojny*, transl. J. Zawadzki, Hachette, Warszawa 2009.
- Tandoc Jr. E.C., Lim Z.W., Ling R., “Defining ‘Fake News’: A Typology of Scholarly Definitions”, *Digital Journalism*, vol. 6, no. 2 (2018), pp. 137–153, <https://doi.org/10.1080/21670811.2017.1360143>.
- “Twitter będzie blokował reklamy polityczne. Dorsey kpi ze stanowiska Facebooka”, *Wirtualne Media*, 31.10.2019, [on-line:] <https://www.wirtualnemedial.pl/arttykul/twitter-bedzie-blokowal-reklamy-polityczne-dorsey-kpi-ze-stanowiska-facebook>.
- “Twitter Transparency Center”, [on-line:] <https://transparency.twitter.com/>.
- Wasiuta O., “Geneza pojęcia i zmiany podejścia do wojny hybrydowej w zachodnim dyskursie politycznym i wojskowym”, *Przegląd Geopolityczny* 2016, no. 17, pp. 26–40.



INFORMATION SECURITY POLICY:  
Conditions, Threats and Implementation  
in the International Environment, pp. 35–51  
<https://doi.org/10.12797/9788381388276.02>

AGNIESZKA NITSZKE 

*Jagiellonian University in Kraków*  
*Team Europe*

## The European Union versus Russian Disinformation

**ABSTRACT:** The war in Ukraine has made public opinion and policy makers aware of the Russian Federation as a major threat to international security, but also to the internal security of the European Union. The military threat is only one of the instruments used by this state. For years, a different type of Russian activity in the EU has been observed, consisting in creating an alternative picture of the situation in Ukraine, and interfering in political processes in selected countries. All these activities are aimed at undermining the cohesion and solidarity of the EU, which, from Moscow's perspective, is a threat to its political interests as a result of the Union's promotion of democratic values and principles and human rights in the international environment. The article presents selected disinformation campaigns carried out by Russia in the EU and then analyses the actions the Union has taken in response. Conclusions and recommendations were formulated in the end.

**KEYWORDS:** European Union, Russia, disinformation, propaganda

## Introduction

The Russian Federation has long seen the EU as a threat to its political interest, particularly in politics and security in post-Soviet countries. Democratic governance and guaranteed civil rights and liberties are incompatible with Russia's policies. The European Neighbourhood Policy (ENP), including its East European dimension – the Eastern Partnership, are seen by Russian decision-makers as an encroachment into Russia's sphere of influence. For this reason, the Russian Federation – for several years now – has been running a large-scale disinformation campaign in the EU aimed not only at disseminating false information about the current situation in Ukraine, but also at breaking apart the political unity among EU states in terms of their attitude towards Russia's actions. The EU is aware of the danger posed by the campaign and, since 2015, has been operating and developing the East StratCom Task Force (SCTF),<sup>1</sup> whose tasks include running the EUvsDisinfo project.

The objective of this paper is to present the results of the Task Force's actions as well as assess the extent to which member states make use of its experiences and collaborate with it. The following research hypotheses were formulated: H1: the goal of Russian disinformation is to weaken unity among EU member states; H2: the EU has developed effective instruments for combating Russian disinformation; H3: the EU is resistant to Russia's disinformation activities. In order to examine these hypotheses, the following research questions were formulated: Q1: In which areas is Russian disinformation most active?; Q2: What entities/groups is Russian disinformation directed at?; Q3: What are the institutional actions taken by the EU to combat Russian disinformation?; Q4: Does the EU collaborate with member states in combating Russian disinformation? If so, how?; Q5: What are the results of the EU's actions aimed at combating Russian disinformation? The activities of the ESCTF, part of the European External Action Service, will be examined through the lens of classical Easton's systems theory,<sup>2</sup> with the securitisation theory<sup>3</sup> used as an auxiliary

---

<sup>1</sup> There are currently three Task Forces – Eastern (2015), Western Balkans (2017) and Middle East and Africa (2017) (East, Western Balkans, South) with a similar mandate. For the purposes of this study, they will be treated as one project. For more see: "Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany", *Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego* 2021, [on-line:] [https://www.eca.europa.eu/Lists/ECADocuments/SR21\\_09/SR\\_Disinformation\\_PL.pdf](https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_PL.pdf) (13.09.2022).

<sup>2</sup> D. Easton, *The Political System: An Inquiry into the State of Political Science*, Alfred A. Knopf, New York 1953, *passim*.

<sup>3</sup> Ł. Fijałkowski, "Teoria sekurytyzacji i konstruowanie bezpieczeństwa", *Przegląd Strategiczny*, no. 1 (2012), pp. 149–161.

tool. The research will be based on qualitative methods, including – in particular – content analysis and institutional, legal and systemic methods.

## Russian disinformation activities in respect of the European Union

Aside from the US, the EU poses the biggest threat to Russia's ambitions to be a superpower. Due to this, one of the objectives of Russian propaganda for internal and external purposes is to sow disinformation on the EU's political, economic and social situation. Russia undertakes institutional activities to attack the European Union as an organisation and its member states. The purpose is to cause the disintegration of the EU and weaken its potential and impact on international relations to supplant liberal democratic values with its own vision of the international order based on Russian supremacy.

In the late 1990s, Aleksandr Dugin, the chief ideologue of Russian imperial ambitions, wrote [in his book *Foundations of Geopolitics*] that Russia would have to use disinformation, destabilisation and annexation to regain its position as a global empire.<sup>4</sup> With time, Dugin's political thought became the foundation of Russia's state ideology under Putin, and the guidelines formulated in this publication formed the basis for an institutionalised industry of propaganda. In its ideological strife against Western values, Russia operates on many levels and along multiple vectors, making identifying threats and their effective nullification difficult. The development of new technologies and communication platforms gave Russian propaganda specialists new possibilities for impacting societies in EU member states. However, Russia continues to use traditional means such as public statements made by politicians or activities of non-state actors located in third parties and operating as think tanks, NGOs or, more broadly, agents of influence.<sup>5</sup>

---

<sup>4</sup> M. Bukowski, M. Duszczyk (eds), *Gościenna Polska 2022+*, Warszawa 2022, [on-line:] <https://wise-europa.eu/wp-content/uploads/2022/06/Raport-Goscinna-Polska-2022.pdf> (13.09.2022).

<sup>5</sup> Agents of influence are a very broad category that includes both third-country nationals operating in the host country and their own citizens. These are people whose actions, public statements or other activities are aimed at supporting the political or economic goals of a third country, without clearly indicating the principal, which significantly hinders the identification of such a person and counteracting their activities. A similar category are 'useful idiots'. Nevertheless, there is a difference between the two categories. It is the link, or lack thereof, with the intelligence of a third country. The agent of influence acts on the orders of the services of a third country, while the "useful idiot" most often acts for ideological reasons, believing in the rightness of a given case. See: "Terms

Given the specific nature of Russia's actions, this paper will present selected examples of disinformation activities that affect the entire European Union and, as such, are meant to cause political, social and economic destabilisation.<sup>6</sup> Brexit, the first-ever case of a country leaving the union, was one of the most important events for the entire EU in its over 70-year history. The UK's potential in the European Union was based not only on its economy or population, but also on its international position. Together with France, the UK is a permanent member of the UN Security Council and a nuclear power. In this context, the debate over the United Kingdom's exit from the European Union became a matter of international importance and raised the interest of many entities, including the Russian Federation, which realised that it could use this situation to weaken two organisations at once – the European Union and the UK itself. Although it has been six years since the Brexit referendum, from the very start it was clear that, for many observers, external players partially controlled Brexit. To this day, nobody has been held responsible. A report by the British Intelligence and Security Committee of Parliament is a major document that sums up the extent of Russian influence during Brexit.<sup>7</sup>

The document was published in July 2020, although the Committee completed work on it in March 2019. The delay resulted from the conclusions of the document, which included a finding that Russian influences penetrated political life in the UK, and UK intelligence was unable to prevent it effectively. The report further stated that Russia had used various means and instruments to influence the Brexit referendum

---

& Definitions of Interest for DOD Counterintelligence Professional”, *Office of Counterintelligence (DXC) Defense CI & Humint Center Defense Intelligence Agency*, 2.05.2011 [on-line:] [http://www.ncix.gov/publications/ci\\_references/CI\\_Glossary.pdf](http://www.ncix.gov/publications/ci_references/CI_Glossary.pdf), pp. 4–5 (13.09.2022).

<sup>6</sup> Three EU-wide issues have been selected, although disinformation activities often target selected Member States and, as such, may have an indirect impact on the situation across the Union. Russian actions often take the form of indirect influence, such as political and financial support for selected political parties in EU countries, which then become agents of Russia's influence, introducing issues that Moscow cares about into public debates and becoming their natural promoters. In recent years, the most famous examples of such activities are the close ties of the French National Union (fr. *Rassemblement national*, until 2018 under the name of the *National Front*, Fr. *Front national*) Marine Le Pen, Italian Northern League (It. *Lega Nord*) by Matteo Salvini or the Freedom Party of Austria (Ger. *Freiheitliche Partei Österreichs*), headed by Vice-Chancellor Heinz-Christian Strache until 2019. See: F. Wesslau, “Putin's Friends in Europe”, *European Council on Foreign Relations*, 19.10.2016, [on-line:] [https://ecfr.eu/article/commentary\\_putins\\_friends\\_in\\_europe7153/](https://ecfr.eu/article/commentary_putins_friends_in_europe7153/) (24.09.2022); B. Bernat skyi, “How to Stop Russia from Bribing European Politicians”, *Visegrad Insight*, 21.09.2022, [on-line:] <https://visegradinsight.eu/russia-bribe-eu-corruption-ukraine/> (27.09.2022).

<sup>7</sup> Intelligence and Security Committee of Parliament: Russia: Presented to Parliament pursuant to section 3 of the Justice and Security Act 2013 Ordered by the House of Commons to be printed on July 21 2020, [on-line:] [https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721\\_HC632\\_CCS001\\_CCS1019402408-001\\_ISC\\_Russia\\_Report\\_Web\\_Accessible.pdf](https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721_HC632_CCS001_CCS1019402408-001_ISC_Russia_Report_Web_Accessible.pdf) (23.09.2022).

campaign on the side of those advocating for leaving the EU (the 'Leave' campaign).<sup>8</sup> The authors of the report claimed that Russian influences in the UK had become the "new normal" – in particular, in "Londongrad", where many Russians enjoy special influence thanks to their money and the UK intelligence services do nothing to prevent it, thus limiting themselves to mitigating potential damage.<sup>9</sup>

Russia's involvement in the 'Leave' campaign involved the dissemination of disinformation on social media and in traditional media (such as RT or Sputnik). False information on the financial and economic impact of UK's membership in the EU was spread, including the claim that the UK was paying huge sums of money into the EU budget, which could otherwise be used to fund the NHS. Another talking point raised during the campaign was EU's migration policy, which – in the opinion of Brexit supporters – limited their country's sovereignty in terms of accepting the influx of foreign citizens. All these issues were presented to create fear and anxiety in British society and induce citizens to vote for "Leave". Although the report did not authoritatively state that Russian disinformation was a factor that decided the vote, the slim difference between those in favour of (51.89%) and those against (48.11%) leaving the EU<sup>10</sup> means that any influence should be treated as unlawful interference.<sup>11</sup> As a result of the decision made by UK citizens, Article 50 of the Treaty on the European Union was activated, and negotiations on UK's exit from the UK began. The process was formally concluded on February 1, 2020, politically and economically weakening both the EU and the UK.

After this difficult process – sometimes called a 'crisis' – concluded, the EU and the rest of the world had to face another test of unity, solidarity and responsibility related to the start of the COVID-19 pandemic. Again, Russian intelligence services decided to take advantage of this extraordinary situation to sow disinformation. Interestingly, but also concerningly, Russian disinformation activities related to the coronavirus pandemic were correlated with the disinformation disseminated by China in this regard. There is

---

<sup>8</sup> The report has a broader context and analyses Russian influence also in the context of the 2014 Scottish independence referendum. In this case, the conclusions are similar and indicate the involvement of Russia on the side of supporters of Scottish independence, which would weaken and destabilise Great Britain. The main accusation arising from the report is that the British services have failed to act in the following years, despite the awareness that a third country is trying to interfere in the political processes in Great Britain.

<sup>9</sup> Intelligence and Security Committee of Parliament..., p. 15.

<sup>10</sup> "Results and Turnout at the EU Referendum", *The Electoral Commission*, 25.09.2019, [on-line:] <https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/elections-and-referendums/past-elections-and-referendums/eu-referendum/results-and-turnout-eu-referendum> (23.09.2022).

<sup>11</sup> D. Ruy, "Did Russia Influence Brexit?", *Center for Strategic & International Studies*, 21.07.2020, [on-line:] <https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit> (23.09.2022).

no evidence that these activities were planned and coordinated; however, both Russia and China had similar goals. Russia repeated Chinese talking points on the origins of the pandemic, where an American bioweapon attack on China was identified as the potential cause of the outbreak or, depending on the medium disseminating the information, US soldiers were said to be responsible for escalating the epidemic. During the pandemic, Russia attempted to sway other countries to lift the sanctions imposed after the annexation of Crimea by providing material assistance to countries, including Italy, by showing that the EU was unable to protect the health and life of its own citizens effectively. The campaign was given the name “From Russia with Love” in the media. Manipulated images depicting EU flags being taken down from public buildings in Russia and performances of the Russian anthem were shown. Restrictions on travelling were presented as evidence of powerlessness and lack of European solidarity.<sup>12</sup>

Similarly to Brexit, Russia used various media to push its agenda – from statements made by politicians and diplomats (which were then quoted in European media), to RT, Sputnik and social media (where troll farms and bots were used to create and spread false information). Media of dubious credibility, particularly websites, also played a significant role by publishing numerous unverified, often mutually contradictory information about the pandemic, which were then reproduced by traditional and social media.<sup>13</sup> In the context of the hazard posed by the pandemic, claims that the pandemic was “fake” were particularly dangerous as they contested the restrictions imposed on everyday life or promoted treatment methods contrary to medical knowledge. Russian disinformation entered a new phase when COVID-19 vaccines were introduced.<sup>14</sup> Russian narration spread in European media focused on the side effects of vaccines and questioned the safety of mRNA-based vaccines. Russian disinformation also attempted to spread social polarisation by raising the issue of mandatory vaccination.<sup>15</sup>

---

<sup>12</sup> P. Śledź, “Ostry cień mgły: antyzachodnia dezinformacja ze strony Chin i Rosji w związku z pandemią COVID-19”, *Rocznik Strategiczny*, vol. 26 (2020/21), pp. 389–401, [on-line:] [https://wnpism.uw.edu.pl/wp-content/uploads/2021/07/Sledz\\_Ostry\\_cien\\_mgly.pdf](https://wnpism.uw.edu.pl/wp-content/uploads/2021/07/Sledz_Ostry_cien_mgly.pdf) (23.09.2022).

<sup>13</sup> R. Reczkowski, “Geopolityczna rozgrywka pandemią COVID-19: rosyjski ekosystem dezinformacji i propagandy”, *Świat Idei i Polityki*, vol. 19 (2020), pp. 251–252, [on-line:] [https://www.ukw.edu.pl/download/58289/12.\\_Robert\\_Reczkowski.pdf](https://www.ukw.edu.pl/download/58289/12._Robert_Reczkowski.pdf) (12.09.2022).

<sup>14</sup> While the development of vaccines against Covid-19 was underway, Russian disinformation was aimed at undermining the effectiveness and safety of the vaccines. It was only after the Russians developed and approved the Sputnik V vaccine that the campaign to discredit vaccines was limited, because some of the negative message to the West returned to Russia and discouraged Russians from vaccinating, see: P. Śledź, *op. cit.*, p. 397.

<sup>15</sup> M. Fraser, “Eksperci: rosyjska dezinformacja antyszczepionkowa rośnie w siłę wraz z wariantem Delta”, *CyberDefence24*, 9.08.2021, [on-line:] <https://cyberdefence24.pl/eksperti-rosyjska-dezinformacja-antyszczepionkowa-rosnie-w-sile-wraz-z-wariantem-delta> (23.09.2022).

Although different, the two examples of Russian disinformation discussed above had the same objective: undermining unity and solidarity on the level of states and communities. Activities related to Brexit laid bare the dangerous mechanism of creating and using agents of influence among political, economic and social elites. This helps lend credence to the message that the Russian Federation wants to spread. This mechanism is still being developed and used – as exemplified by disinformation activities surrounding the conflict in Ukraine.

Narration on the situation in Ukraine can be divided into two phases, each with a different dynamic. The first phase began in 2013 and was related to another attempt at bringing Ukraine closer to the EU. The Euromaidan confirmed that Ukraine was on a pro-European course which the Russian Federation wouldn't accept. 2014 saw the first stage of Russia's political and military operation against Ukraine begin, resulting in the annexation of Crimea and the outbreak of hostilities in the Donbas. The international democratic community condemned Russia's action and refused to recognise the resulting territorial changes. The EU was one of the entities who reacted to Russia's illegal actions by imposing a number of economic and political sanctions.<sup>16</sup> From the beginning of the conflict, Russia used multiple channels – political (Ministry of Foreign Affairs), diplomatic (diplomatic missions in third countries and international organisations), traditional and social media – to wage a massive campaign disparaging Ukraine and Ukrainians. Ukraine's right to sovereignty was undermined, with the country being described as a „failed state” or “artificial creation”. Another trend in narration pointed to the historical background by saying that Ukraine was an integral part of the Russian Federation. Legal pro-European and democratic authorities of Ukraine were called a „Nazi junta” that was a threat to the Russian-speaking population of Ukraine. The importance and political influence of nationalist parties were exaggerated to show that the danger posed by Nazis was real. Yet another narrative was

---

<sup>16</sup> As of March 3, 2014, EU institutions: The European Council, the Council of the EU and the European Commission worked on sanctions against the Russian Federation in connection with the aggression against Ukraine. Entry bans were introduced for Russian officials and trade restrictions were imposed. The cancellation of the EU-Russia summit in Sochi scheduled for June 2014 and the suspension of visa talks and a new strategic agreement were also politically significant. For a complete calendar of sanctions imposed by the EU on the Russian Federation, see: “Kalendarium – sankcje UE wobec Rosji w sprawie Ukrainy”, *Strona Rady Europejskiej i Rady Unii Europejskiej*, [on-line:] <https://www.consilium.europa.eu/pl/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/> (12.09.2022).

used to show Ukraine as an agent of the West and the US, who would be in a good position to endanger the safety of Russia by taking over its neighbour.<sup>17</sup>

Attempts were made to use the media to legalise the occupation of Ukraine by introducing the name “Federal Republic of Novorossiya” into the public sphere. Ultimately, “Novorossiya” was meant to encompass the entire south of Ukraine.<sup>18</sup> This was not only an attempt to familiarise the public opinion with the new name, but, most of all, preparation for an escalation of the aggression and new status quo. An important goal of disinformation, in this case, was to reach the political decision-makers in the EU as their position would determine the scale of sanctions to be imposed on Russia for violating international law and the territorial integrity of a sovereign country. Due to this, an increase in relations between certain political parties active in EU member states and the Russian Federation could be observed at the time.

These parties could primarily be described as nationalist and populist. Their common trait was their potential. By using the concept of political relevance of a party, as proposed by Giovanni Sartori, these parties were (and still are) those with the potential to use political blackmail and rarely become part of a coalition. Pro-Russian circles in France (Marine Le Pen’s National Rally), Italy (Lega Nord) or Hungary (Fidesz) were strengthened in this way. This is a form of political capital which firstly helps with disinformation as politicians of these parties push Russian narration, and secondly weakens the unity of the EU and, as a result, its potential. Although public opinion and mainstream media lost interest in the situation in Ukraine after 2015, disinformation campaigns did not stop and continued to be pushed – primarily in Russian media that reached international audiences (Sputnik, RT) and social media. The aim was to prepare the international public for the next stage of the conflict, which began in February 2022. The same narration as before was used and further strengthened, describing Ukraine as a fascist/Nazi state.<sup>19</sup>

---

<sup>17</sup> F. Bryjka, “Rosyjska dezinformacja na temat ataku na Ukrainę”, *Polski Instytut Spraw Międzynarodowych*, 25.02.2022, [on-line:] <https://www.pism.pl/publikacje/rosyjska-dezinformacja-na-temat-ataku-na-ukraine> (15.09.2022).

<sup>18</sup> A. Włodkowska-Bagan, “Rosyjska ofensywa propagandowa. Casus Ukrainy”, *Studia Polilogiczne*, vol. 49 (2018), pp. 109–124, [on-line:] <http://www.studiapolilogiczne.pl/pdf-115451-44713?filename=RUSSIAN%20PROPAGANDA.pdf> (12.09.2022).

<sup>19</sup> As early as January 20, 2022, the US State Department published a document identifying the seven main lies of Russian propaganda about Ukraine: 1. Ukraine is the aggressor; 2. The West is pushing Ukraine towards conflict; 3. Russian troop movements are mere manoeuvres on their own territory; 4. The US is planning a chemical attack in the Donbas; 5. Russia defends its own citizens on the territory of Ukraine; 6. NATO has broken the non-enlargement agreement and intends to accept Ukraine; 7. The West does not want to talk, it just starts imposing sanctions. American services prepared a report based on an analysis of materials published mainly in American media, but

A new element of the programme was a campaign aimed personally at Volodymyr Zelenskyy, President of Ukraine, who has Jewish roots. The president's Jewish roots were somehow not incompatible with his alleged Nazi beliefs. The objective of the disinformation campaign was to convince the public that Russia was conducting a „special operation” aimed at protecting the Ukrainian people from their government. New themes were introduced in later weeks and months: Ukrainian refugees, armed hostilities and their consequences, and nuclear safety. Ukrainian refugees were depicted as a problem and danger to European societies. Narratives were very diverse and focused on such themes as the economy (a burden to social systems and health care) and morality (women refugees from Ukraine as a threat to marriages).<sup>20</sup>

Of particular importance to Russian propaganda is the depiction of military action and its own explanations for gradually uncovering war crimes. The dominant theme coincides with the Kremlin's official line that the crimes were a sham aimed at discrediting the Russian army or that the Ukrainians themselves committed the crimes. Since the beginning of the war, potential contamination due to radiation has been an important theme. This context involves two narratives, the first – related to the potential use of tactical nukes by Russia, which the Kremlin propaganda depicts as a manifestation of Russia's right to defend its own interest, and the second – related to the potential intentional causing of a failure at one of the nuclear power plants in Ukraine or attacking it. Russians have taken over the largest Ukrainian nuclear plant in Zaporizhzhia, and the situation around that facility has been the subject of a disinformation campaign ever since. After the experiences related to the Chernobyl disaster, the topic is of particular interest to the public – which Russia has been taking full advantage of. The danger posed to the European security system by threats related to the war in Ukraine is unprecedented. The scale of disinformation is far beyond the previously described examples of Russia's interference with the internal affairs of the EU during Brexit and the pandemic.

---

the narrative was global and the same topics and lies were repeated around the world. See: “Fact vs. Fiction: Russian Disinformation on Ukraine”, *US Department of State*, 20.01.2022, [on-line:] <https://www.state.gov/fact-vs-fiction-russian-disinformation-on-ukraine/> (23.09.2022).

<sup>20</sup> These theses were often adopted and copied by the media and opinion-forming centres in the EU Member States, e.g. in one of the analyses of the Jagiellonian Club, see.: M. Gulczyński, “To przez te Ukrainki? Szkoła, praca, lekarz, mieszkanie. Polki pod presją zwrócą się ku prawicy?”, *Klub Jagielloński*, 20.04.2022, [on-line:] <https://klubjagiellonski.pl/2022/04/20/to-przez-te-ukrainki-szkola-praca-lekarz-mieszkanie-polki-pod-presja-zwroca-sie-ku-prawicy/> (23.09.2022).

## The EU's activities in response to Russian disinformation

The European Union is in a difficult situation when attempting to fight Russian disinformation and propaganda. Firstly, as an entity aspiring to be a normative power, it cannot use the same instruments as Russia as they are incompatible with its rules and values. Secondly, its ability to use other available instruments is significantly limited. Member states did not grant the EU competencies in respect of internal security. According to Article 72 of the treaty on the functioning of the European Union (TFEU), responsibilities concerning the maintenance of law and order and the safeguarding of internal security lie with the member states.<sup>21</sup>

Member states may cooperate in this regard, with the EU coordinating the cooperation. The Standing Committee on Operational Cooperation on Internal Security plays a particularly important role in this aspect (Article 71 of TFEU).<sup>22</sup> In addition, matters related to the disinformation activities of the Russian Federation in the EU combine elements of internal and external security as they involve a third country whose actions affect internal political, economic and social processes in the EU and its member states. Despite the legal and political limitations in becoming involved in actions related to security policy, the EU has developed and continues to develop mechanisms aimed at counteracting Russian disinformation. Most importantly, the EU defined disinformation as “verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm. Disinformation does not include reporting errors, satire and parody, or clearly identified partisan news and commentary”.<sup>23</sup>

This definition allows for some possibility of the continued impact of propaganda and dissemination of controlled information but should be treated as an attempt to reconcile the protection of public interest and a guarantee of the fundamental value of free speech.

The EU had already taken specific action in response to Russian disinformation in 2015. At a session of the European Council, leaders of member states tasked the High Representative of the Union for Foreign Affairs and Security Policy (HR/VP) with preparing a plan for fighting Russian disinformation. They noted that a special

---

<sup>21</sup> *Traktat o funkcjonowaniu Unii Europejskiej*, Dz.U. UE C 326 z 26.10.2012, p. 74.

<sup>22</sup> *Ibidem*.

<sup>23</sup> COM(2018)236 final, 26.04.2018, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach*, p. 4.

unit should be created to implement tasks related to counteracting disinformation. This became the basis for creating the StratCom Task Force on September 1, 2015.<sup>24</sup>

Due to the previously discussed treaty limitations, as well as the fact that the HR/VP was designated as the entity responsible for this matter, the Task Force was organised within the European External Action Service (EEAS). This is where it became part of Strategic Communication, Task Forces and Information Analysis Division (AFFGEN.7), which also includes a horizontal team tasked with analysing potential threats to EU's security system, creating the backbone of the EU's early disinformation warning system. SCTF initially operated in a very limited scope as it had only nine members and was funded from voluntary payments made by member states. However, when it became clear that Russian disinformation activity was posing a constantly growing threat, a decision was made in 2018 that funding would be granted by the European Parliament. The Task Force's responsibilities were made more specific, and it was made more powerful with the adoption of two documents by the EU: "Tackling online disinformation: a European Approach"<sup>25</sup> and "On the European democracy action plan".<sup>26</sup>

Three areas of combating disinformation were identified: firstly, making the EU's own communication more effective to ensure a better flow of verified and credible information, in particular on EU-Ukraine relations, thus eliminating the potential for reproducing false information; secondly, strengthening free and independent media to guarantee that an accurate image of the world will be shown; thirdly, raising awareness of the disinformation problem – its forms and effects among citizens, political decision-makers and EU institutions, as well as in member states and countries affiliated with the EU.<sup>27</sup>

Major responsibilities of the Task Force include media monitoring – both traditional and social media – to track and counteract Russian disinformation. The group monitors media in all member states. Due to this, coordination of its activities with relevant national intelligence services is required. The group analyses reported content

---

<sup>24</sup> "Conclusions of the European Council, 19–20 March 2015", Brussels, *EUCO* 11/15, 20.03.2015, [on-line:] <https://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/pl/pdf> (12.09.2022).

<sup>25</sup> COM(2018) 236 final, 26.04.2018, pp. 1–20.

<sup>26</sup> COM(2020) 790 final, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions On the European democracy action plan*, Brussels, 3.12.2020, pp. 1–31.

<sup>27</sup> "Przeciwstawianie się trwającym kampaniom dezinformacyjnym prowadzonym przez Rosję: Historia EUvsDisinfo", *EUvsDisinfo*, 20.04.2020, [on-line:] <https://euvsdisinfo.eu/pl/przeciwstawianie-sie-trwajacym-kampaniom-dezinformacyjnym-prowadzonym-przez-rosje-historia-euvsdisinfo/> (12.09.2022).

to prepare guidelines for interested entities on which content presents a potential threat. Education is an important part of the Task Force's responsibilities to ensure that various groups – citizens, media or political decision-makers can independently make a credible judgment as to the veracity of the information they obtain. These tasks are implemented as part of the EUvsDisinfo project.<sup>28</sup>

The project involves an ongoing analysis of media in 15 languages. The objective is to expose content republished in European media from Russian pro-Kremlin outlets. The geographical scope of the analysis also includes the Eastern Partnership, West Balkans and EU's Southern neighbourhood because they are a particular target for disinformation activity and attempts at interfering with political life, which may – in turn – lead to a destabilisation of the EU's closest neighbours. EUvsDisinfo's activities – focused on monitoring the situation in these countries – are, therefore, of key importance for European security.

EUvsDisinfo is an open platform, meaning that any interested entity may use the information found on it. It includes a database of over 12,000 examples of disinformation content, which is updated on an ongoing basis. It's worth noting that information gathered in the database is developed to identify main threats and their evolution to facilitate defence against such content. Although disinformation content concerning Ukraine has been the project's main focus since 2015, Russian propaganda – as already noted earlier in the paper – uses various topics to destabilise the EU and its member states. Due to this, the themes tackled by the platform focus on several issues: Ukraine, the COVID-19 pandemic, elections, climate change, conspiracy theories and other content.<sup>29</sup>

The threat posed by Chinese disinformation has also been noted, and content originating from this country that is potentially detrimental to public life in the EU is also subject to analysis. The actions of StratCom have met with much praise, both from European and foreign decision-makers and experts. The methodology of analysis of disinformation and real contribution to counteracting this phenomenon has been recognised.<sup>30</sup> However, this does not mean that no criticism has been forthcoming. Some of the criticism has been levelled not against the unit itself, but on the method

---

<sup>28</sup> Website *EUvsDiSiNFO*, [on-line:] <https://euvsdisinfo.eu/> (23.09.2022).

<sup>29</sup> “Przeciwstawianie się trwającym kampaniom...”

<sup>30</sup> See: T. Glavin, “How Russia's Attack on Freeland Got Traction in Canada”, *McLeans*, 14.03.2017, [on-line:] <https://www.macleans.ca/politics/how-russias-attack-on-freeland-got-traction-in-canada/> (23.09.2022); M. Scott, M. Eddy, “Europe Combats a New Foe of Political Stability: Fake News”, *The New York Times*, 20.02.2017 [on-line:] <https://www.nytimes.com/2017/02/20/world/europe/europe-combats-a-new-foe-of-political-stability-fake-news.html> (23.09.2022).

of its organisation – which lies with the competencies of EU institutions and member states. In the opinion of those critical of the Task Force, while its overall impact has been positive, adequate funding for the initiative that would enable it to reach its full potential has not been secured.<sup>31</sup> This, however, has been gradually changing. In 2018, thanks to funds provided by the European Parliament, StratCom's budget was €1.1m. The budget was gradually increased in the following years to €3m in 2019 and €4m in 2020. In 2021, it reached a record level of €11.1m.<sup>32</sup>

As already noted, the EU itself is not competent to adopt binding acts of law to regulate issues related to the systemic fight against disinformation due to the division of competencies between the EU and its member states as laid down in treaties. Due to this, the EU's actions in this area are of a supporting and coordinating nature. Acting according to treaties and within its competencies, the EU cooperated with member states to identify threats related to escalating disinformation – originating primarily in Russia, but with an increasing contribution from China – and has taken actions aimed primarily at supporting services in member states responsible for ensuring security and maintaining public order. Creating the East StratCom unit was an important step but has been insufficient given the scale of disinformation attacks. Actions must be taken on the level of member states and coordinated. One of the proposals put forward in this regard is the creation of a network of national StratCom units. In December 2018, the European Council approved a plan to create an early disinformation warning system – the Rapid Alert System (RAS), which was implemented in March of the following year. RAS is an interactive platform that connects national points of contact,<sup>33</sup> tasked with enabling member states to inform each other of disinformation campaigns and share analysis and reports concerning this issue. The platform aims to facilitate the development and implementation of a coordinated response of all member states to identified threats. It is stressed that the tool is meant to help

---

<sup>31</sup> M. Apuzzo, "Top EU Diplomat Says Disinformation Report Was Not Watered Down for China", *The New York Times*, 30.05.2020 [on-line:] <https://www.nytimes.com/2020/04/30/world/europe/coronavirus-china-eu-disinformation.html> (23.09.2022).

<sup>32</sup> "Questions and Answers about the East StratCom Task Force", *European External Action Service*, [on-line:] [https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force\\_en](https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en) (23.09.2022). According to the European Court of Auditors, in 2015-2020, the total EU expenditure on combating disinformation amounted to EUR 50 million, dispersed in various EU programmes and activities. "Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany", p. 4.

<sup>33</sup> In Poland, it is a special department for strategic communication at the Ministry of Foreign Affairs (StratCom), F. Bryjka, "Rozwój unijnych zdolności do zwalczania zagrożeń hybrydowych", *Polski Instytut Spraw Międzynarodowych*, 1.08.2022, [on-line:] <https://pism.pl/publikacje/rozwoj-unijnych-zdolnosci-do-zwalczania-zagrozen-hybrydowych>, p. 4 (12.09.2022).

member states save time and money they would otherwise have to spend were they all to individually engage in the constant observation and reacting to disinformation activities. Another benefit is the ability to develop more effective instruments in the fight against disinformation. The mechanism of operation of the platform was made as simple as possible: EU institutions and national points of contact enter data into the system, and EEAS and the European Council analyse and investigate them.<sup>34</sup> The EU also uses other instruments to limit the area of effect of Russian disinformation. As part of its activities related to imposing sanctions on the Russian Federation for its attack on Ukraine, on March 2, 2022, the European Council urgently suspended the broadcasting activities of the Sputnik agency and RT stations (RT English, RT UK, RT Germany, RT France and RT Spanish).<sup>35</sup>

## Summary

The three selected examples of Russian disinformation campaigns discussed in the paper – related to Brexit, COVID-19 pandemic and the war in Ukraine – clearly show that a politically, socially and economically united and consolidated EU is treated by the Kremlin as an enemy. Due to this, Russia is attempting to destroy this unity which was partially successful in the examples discussed in the paper. In the case of Brexit, as noted in the report of the Committee of the British Parliament, there is no hard data confirming that the disinformation campaign itself affected the results of the referendum, but the existence of close ties, including financial ones, between Russia and leaders of the ‘Leave’ campaign was confirmed. UK’s exit from the European Union was undoubtedly beneficial to Russia as it weakened both the EU and the UK in political and economic terms. The example of the COVID-19 pandemic is different as the main objective of disinformation, in this case, was to create divisions within societies, push conspiracy theories and, as a result, create a threat to the life and health of EU citizens. In addition, Russia attempted to use the crisis caused by the pandemic to achieve political goals. Using so-called “face mask politics”, the Kremlin wanted to improve its image and cause sanctions imposed after its annexation of Crimea in

---

<sup>34</sup> *Rapid Alert System*, Factsheet, March 2019, [on-line:] [https://www.eeas.europa.eu/sites/default/files/ras\\_factsheet\\_march\\_2019\\_0.pdf](https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf) (23.09.2022).

<sup>35</sup> “EU Imposes Sanctions on State-owned Outlets RT/Russia Today and Sputnik’s Broadcasting in the EU”, *European Council and Council of the European Union*, [on-line:] <https://www.consilium.europa.eu/pl/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/> (23.09.2022).

2014 to be lifted. In this case, Russia could not achieve its political goals, even though voices supporting lifting the sanctions could be heard in some countries (e.g., Hungary or Austria). The campaign aimed at besmirching Ukraine's image in the EU is the most difficult to assess as it has been going on the longest. The first phase of the war, which commenced in 2014, resulted in the EU implementing institutionalised action aimed at protecting its citizens, public institutions and media against manipulated information. The development of the StratCom task force and the RAS project, in combination with the Commission's communication specifying priorities in fighting disinformation, have created a foundation on which an effective system can be built to combat Russian disinformation.

The first of the research hypotheses formulated at the beginning of the paper, concerning Russia's disinformation in the EU, has been confirmed. The second and third hypotheses have been partially confirmed: instruments developed so far to fight Russian disinformation have been able to limit its impact but not fully eliminate it, making the EU more resilient to disinformation attacks when compared to other countries with additional actions required to further strengthen institutional and systemic solutions.

A number of conclusions can be made based on the issues discussed: firstly, a strong and united European Union is Russia's rival; secondly, Russia's activities aimed at destabilising the EU will be primarily focused on medium- and small-sized countries where anti-EU sentiment will be encouraged; thirdly, after the elimination of its main communication channels – Sputnik and RT – from the European market, Russia will search for new instruments to influence public opinion in the EU. In summary, only a strong and united EU that avoids internal conflict and is based on democratic values will be able to effectively fight disinformation and protect its member states against Russian influence.

## References

- Apuzzo M., "Top EU Diplomat Says Disinformation Report Was Not Watered Down for China", *The New York Times*, 30.05.2020 [on-line:] <https://www.nytimes.com/2020/04/30/world/europe/coronavirus-china-eu-disinformation.html>.
- Bernatskyi B., "How to Stop Russia from Bribing European Politicians", *Visegrad Insight*, 21.09.2022, [on-line:] <https://visegradinsight.eu/russia-bribe-eu-corruption-ukraine/>.
- Bryjka F., "Rosyjska dezinformacja na temat ataku na Ukrainę", *Polski Instytut Spraw Międzynarodowych*, 25.03.2022, [on-line:] <https://www.pism.pl/publikacje/rosyjska-dezinformacja-na-temat-ataku-na-ukraine>.

- Bryjka F., "Rozwój unijnych zdolności do zwalczania zagrożeń hybrydowych", *Polski Instytut Spraw Międzynarodowych*, 1.08.2022, [on-line:] <https://pism.pl/publikacje/rozwoj-unijnych-zdolnosci-do-zwalczania-zagrozen-hybrydowych>.
- Bukowski M., Duszczyk M. (eds), *Gościenna Polska 2022+*, Warszawa 2022, [on-line:] <https://wise-europa.eu/wp-content/uploads/2022/06/Raport-Goscienna-Polska-2022.pdf>.
- COM(2018)236 final of 26/04/2018, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling online disinformation: a European Approach*.
- COM(2020) 790 final, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions On the European democracy action plan*, Brussels, 3.12.2020.
- "Conclusions of the European Council, 19–20 March 2015", Brussels, *EUCO 11/15*, 20.03.2015, [on-line:] <https://data.consilium.europa.eu/doc/document/ST-11-2015-INIT/pl/pdf>.
- "Dezinformacja w UE – pomimo podejmowanych wysiłków problem pozostaje nierozwiązany", *Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego*, 2021, [on-line:] [https://www.eca.europa.eu/Lists/ECADocuments/SR21\\_09/SR\\_Disinformation\\_PL.pdf](https://www.eca.europa.eu/Lists/ECADocuments/SR21_09/SR_Disinformation_PL.pdf).
- Easton D., *The Political System: An Inquiry into the State of Political Science*, Alfred A. Knopf, New York 1953.
- "EU Imposes Sanctions on State-owned Outlets RT/Russia Today and Sputnik's Broadcasting in the EU", *European Council and Council of the European Union*, 2.03.2022, [on-line:] <https://www.consilium.europa.eu/pl/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/>.
- "Fact vs. Fiction: Russian Disinformation on Ukraine", *US Department of State*, 20.01.2022, [on-line:] <https://www.state.gov/fact-vs-fiction-russian-disinformation-on-ukraine/>.
- Fijałkowski Ł., "Teoria sekurytyzacji i konstruowanie bezpieczeństwa", *Przegląd Strategiczny*, no. 1 (2012), pp. 149–161, <https://doi.org/10.14746/ps.2012.1.10>.
- Fraser M., "Eksperci: rosyjska dezinformacja antyszczepionkowa rośnie w siłę wraz z wariantem Delta", *CyberDefence24*, 9.08.2021, [on-line:] <https://cyberdefence24.pl/eksperci-rosyjska-dezinformacja-antyszczepionkowa-rosnie-w-sile-wraz-z-wariantem-delta>.
- Glavin T., "How Russia's Attack on Freeland Got Traction in Canada", *McLean's*, 14.03.2017, [on-line:] <https://www.macleans.ca/politics/how-russias-attack-on-freeland-got-traction-in-canada/>.
- Gulczyński M., " 'To przez te Ukrainki? Szkoła, praca, lekarz, mieszkanie. Polki pod presją zwrócą się ku prawicy?'", *Klub Jagielloński*, 20.04.2022, [on-line:] <https://klubjagiellonski.pl/2022/04/20/to-przez-te-ukrainki-szkola-praca-lekarz-mieszkanie-polki-pod-presja-zwroca-sie-ku-prawicy/>.
- Intelligence and Security Committee of Parliament: Russia: Presented to Parliament pursuant to section 3 of the Justice and Security Act 2013 Ordered by the House of Commons to be printed on July 21 2020, [on-line:] [https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721\\_HC632\\_CCS001\\_CCS1019402408-001\\_ISC\\_Russia\\_Report\\_Web\\_Accessible.pdf](https://isc.independent.gov.uk/wp-content/uploads/2021/01/20200721_HC632_CCS001_CCS1019402408-001_ISC_Russia_Report_Web_Accessible.pdf).
- "Kalendarium – sankcje UE wobec Rosji w sprawie Ukrainy", *Strona Rady Europejskiej i Rady Unii Europejskiej*, [on-line:] <https://www.consilium.europa.eu/pl/policies/sanctions/>

- restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/.
- “Questions and Answers about the East StratCom Task Force”, *European External Action Service*, [on-line:] [https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force\\_en](https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en).
- “Przeciwstawianie się trwającym kampaniom dezinformacyjnym prowadzonym przez Rosję: Historia EUvsDisinfo”, *EUvsDisinfo*, 20.04.2020, [on-line:] <https://euvsdisinfo.eu/pl/przeciwstawianie-sie-trwajacym-kampaniom-dezinformacyjnym-prowadzonym-przez-rosje-historia-euvsdisinfo/>.
- Rapid Alert System*, March 2019, [on-line:] [https://www.eeas.europa.eu/sites/default/files/ras\\_factsheet\\_march\\_2019\\_0.pdf](https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf).
- Reczkowski R., “Geopolityczna rozgrywka pandemią COVID-19: rosyjski ekosystem dezinformacji i propagandy”, *Świat Idei i Polityki*, vol. 19 (2020), [on-line:] [https://www.ukw.edu.pl/download/58289/12\\_Robert\\_Reczkowski.pdf](https://www.ukw.edu.pl/download/58289/12_Robert_Reczkowski.pdf).
- “Results and Turnout at the EU Referendum”, *The Electoral Commission*, 25.09.2019, [on-line:] <https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/elections-and-referendums/past-elections-and-referendums/eu-referendum/results-and-turnout-eu-referendum>.
- Ruy D., “Did Russia Influence Brexit?”, *Center for Strategic & International Studies*, 21.07.2020, [on-line:] <https://www.csis.org/blogs/brexit-bits-bobs-and-blogs/did-russia-influence-brexit>.
- Scott M., Eddy M., “Europe Combats a New Foe of Political Stability: Fake News”, *The New York Times*, 20.02.2017, [on-line:] <https://www.nytimes.com/2017/02/20/world/europe/europe-combats-a-new-foe-of-political-stability-fake-news.html>.
- Śledź P., “Ostry cień mgły: antyzachodnia dezinformacja ze strony Chin i Rosji w związku z pandemią COVID-19”, *Rocznik Strategiczny*, vol. 26 (2020/21), pp. 389–401, [on-line:] [https://wnpism.uw.edu.pl/wp-content/uploads/2021/07/Sledz\\_Ostry\\_cien\\_mgly.pdf](https://wnpism.uw.edu.pl/wp-content/uploads/2021/07/Sledz_Ostry_cien_mgly.pdf).
- “Terms & Definitions of Interest for DOD Counterintelligence Professional”, *Office of Counterintelligence (DXC) Defense CI & Humint Center Defense Intelligence Agency*, 2.05.2011, [on-line:] [http://www.ncix.gov/publications/ci\\_references/CI\\_Glossary.pdf](http://www.ncix.gov/publications/ci_references/CI_Glossary.pdf).
- “Timeline – EU Restrictive Measures against Russia over Ukraine”, *European Council and Council of the European Union*, [on-line:] <https://www.consilium.europa.eu/pl/policies/sanctions/restrictive-measures-against-russia-over-ukraine/history-restrictive-measures-against-russia-over-ukraine/>.
- Treaty on the functioning of the European Union, OJ UE C 326 of 26/10/2012.
- Wesslau F., “Putin’s Friends in Europe”, *European Council on Foreign Relations*, 19.10.2016, [on-line:] [https://ecfr.eu/article/commentary\\_putins\\_friends\\_in\\_europe7153/](https://ecfr.eu/article/commentary_putins_friends_in_europe7153/).
- Włodkowska-Bagan A., “Rosyjska ofensywa propagandowa. Casus Ukrainy”, *Studia Polito-logiczne*, vol. 49 (2018), pp. 109–124, [on-line:] <http://www.studiapolitologiczne.pl/pdf-115451-44713?filename=RUSSIAN%20PROPAGANDA.pdf>.



# Information Security and Mechanisms Used by the Russian Federation to Shape Polish Public Opinion

**ABSTRACT:** The article presents the results of research on the determinants of information security and the disinformation activity of the Russian side – which relates to the implementation of the objectives of the foreign policy of the Russian Federation concerning Poland, but also other countries in the region of Central and Eastern Europe. The article presents trends, methods of operation and techniques used by the Russians that have been implemented in recent years and the recent period. The text also outlines the general features of disinformation activities and propaganda, the main narratives and the trends in Russian communications.

**KEYWORDS:** information security, propaganda, disinformation

## Introduction

As part of this work, an attempt will be made to describe the determinants of information security and disinformation activity Russia, referring to the pursuit of foreign policy objectives of the Russian Federation concerning Poland, but also countries in the region such as Lithuania and Ukraine. The following analysis will outline the trends, modus operandi and techniques employed by the Russian side that were mani-

fested primarily in 2021. Based on specific examples of actions, the general features of disinformation activities conducted against countries in the region by the Russian Federation and the main narratives, as well as the orientations of Russian communications, will be presented. The main goal of the research on the issue discussed [in the paper] will be to present the methods and techniques used by the Russian part in attempts to influence Polish society. Russian activity refers, however, not only to the formation of Poles' opinions in such a way as to influence Polish domestic policy, but also to gaining the ability to interfere in the foreign policy line of the Polish state after February 2022 – especially in the field of Polish-Ukrainian relations.

At the beginning of the work, the meaning of the key terms that will be expressed in the text should be clarified. The concepts of *disinformation* and *propaganda* in this paper will be captured based on Yevhen Mahda's interpretation, whereby disinformation is "the deliberate dissemination of false information in order to achieve military objectives more effectively and provoke the opponent to take certain actions".<sup>1</sup> The term *propaganda* in this context will be understood as "a form of communication designed to disseminate information intended to influence and create public opinion in accordance with the needs of a particular ideology or so as to serve a particular purpose".<sup>2</sup> *Propaganda* and *disinformation* will, therefore, be understood as part of information and psychological activities. Because of this, at this point, it is worth clarifying the notion of an *information-psychological-oriented operation*, a concise explanation of which was provided by Michał Wojnowski, according to whom "An information-psychological-oriented operation can be defined as a methodology for creating and implementing a combination of various activities leading to the transformation of the image of the world that exists in the consciousness of the opposing party".<sup>3</sup> Another concept that will arise at work will be *narration*. It will be understood as a "story" that is part of a "way of understanding reality".<sup>4</sup> In the context of the issue at hand, it will thus be a means used to create an appropriate – from a Russian perspective – vision of reality.

---

<sup>1</sup> Є. Магда, *Гібридна агресія Росії: Уроки для Європи*, Калмар, Київ 2017, p. 263.

<sup>2</sup> *Ibidem*.

<sup>3</sup> M. Wojnowski, "Zarządzanie refleksyjne jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.", *Przegląd Bezpieczeństwa Wewnętrznego*, vol. 7 (2015), p. 16.

<sup>4</sup> J. Trzebiński, *Narracja jako sposób rozumienia świata*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2002, p. 13.

## Methods of interference by the Russian Federation in Poland's infosphere

In pursuing its foreign policy objectives, the Russian Federation actively uses information tools to form attitudes in the societies attacked that are appropriate from its perspective. Through a network of influence centres tailored to the societies in question, information operations are carried out to elicit the reactions assumed by the Russian Federation, which are a necessary element of achieving the Russian Federation's tactical and strategic objectives. It is worth remembering that the objectives of the Russian Federation refer both to individual states and international structures.

In the case of countries such as Poland, Lithuania and Ukraine, the objectives pursued by the Russians relate to destabilising the socio-political situation, stimulating anti-EU, anti-NATO and anti-American attitudes and stimulating tensions between the countries mentioned above (e.g., between Poland and Ukraine, or Poland and Lithuania). The above activity of the Russian side refers to the attempts to disintegrate NATO and the EU. As for each of the countries identified, the Russian party has clearly defined objectives, which are pursued in the information sphere with clear consideration of the country's cultural, political and economic specifics. By influencing a given society, the Russian Federation uses the infrastructure it owns, which it has acquired as part of the long-term formation of its influence capabilities. In the case of the Polish public, the Russian side cannot count on the possibility of a serious impact on society through Russian-speaking sources. One group that can be directly influenced by broadcasting Russian-language materials (TV programmes broadcast from the territory of the Russian Federation or key news portals) is a serious group of economic migrants who came to Poland from Ukraine (before February 24, 2022), Belarus or Russia (up to 3 million people – the estimated number of economic migrants relating to the number of work permits issued in 2021)<sup>5</sup> and some Ukrainian refugees who arrived after February 24, 2022. However, these groups do not seem to be strongly influenced by Russian disinformation messages – the narratives about Poland are contrasted with reality, so the harmful charge seems to be partially neutralised.

At present, however, the penetration of narratives similar to Russian propaganda into the Polish infosphere through groups operating in social networks (especially Facebook) is clearly observed. Some of these groups, run in parallel in Polish and Rus-

---

<sup>5</sup> “Rekordowa liczba imigrantów zarobkowych w Polsce. Niezaspokojony popyt”, *Rzeczpospolita*, 25.01.2022 [on-line:] <https://www.rp.pl/rynek-pracy/art19323661-rekordowa-liczba-imigrantow-zarobkowych-w-polsce-niezaspokojony-popyt> (1.09.2022).

sian (probably administered by people coming from areas of the Russian Federation or Belarus), become sources that enable Poles to obtain disinformation or propaganda content. These materials are often pro-Russian (building a positive image of Russia and Russian politicians) and anti-Ukrainian (portraying Ukraine as a “force of evil”, a country of chaos controlled by almost mythical “Banderites”). The aforementioned groups and openly pro-Russian fanpages are also run by Polish citizens and members of organisations registered in Poland, such as “Kursk”<sup>6</sup> or “Polish-Russian Brotherhood”.<sup>7</sup> Such environments, through their activities on social networks (especially Facebook), introduce materials to the Polish infosphere that warm up the image of the Russian Federation and the USSR, and also publish content that is openly anti-Ukrainian and anti-Western. The activity of the groups is part of the context of stimulating anti-Western, anti-Ukrainian, anti-government and pro-Russian public moods. The leaders of the indicated circles cooperate with the Polish-language editors of the Sputnik portal, becoming “experts” in confirming Russian propaganda theses<sup>8</sup> (this process was noticeable until the activities of the Sputnik portal were limited after February 2022).

In the space of social networks, there are also several fanpages that are not openly pro-Russian but are the source responsible for introducing disinformation content to the Polish Internet space. One of the examples of this type of source was a fanpage called “Konflikty i Wiadomości Światowe” [“Conflicts and News of the World”].<sup>9</sup> The indicated source was actively used during the escalation of tensions around the Ukrainian borders at the turn of March and April 2021. “Conflicts and World News” was responsible for stimulating a mood of panic caused by the spectre of impending war and carrying out activities of accusing the Ukrainian side of bearing responsibility for the impending war. In 2022, this function was performed by, among others, “Stop U-krainizacji Polski” group [“Stop the Ukrainisation of Poland”]<sup>10</sup> – which, like many others, started to function as a lobbying group for narratives that undermine the sense of vaccination against Covid-19, and later focused on stimulating hatred against Ukraine

---

<sup>6</sup> Fanpage created by the Kursk Association, over 4.6, [on-line:] <https://www.facebook.com/Stkursk> (1.09.2022).

<sup>7</sup> A group formed by the Polish-Russian Brotherhood, over 7,000 group members, [on-line:] <https://www.facebook.com/groups/baczerozo> (8.09.2022).

<sup>8</sup> Sample text of the Sputnik portal: “Kursk’ o wydaniu ‘Mein Kampf’ w Polsce: Propagowanie totalitaryzmu”, *Sputnik Polska*, 20.01.2021, [on-line:] <https://pl.sputniknews.com/20210120/mein-kampf-po-polsku-kursk-kieruje-sprawe-do-prokuratury-sputnik-13700194.html> (1.09.2022).

<sup>9</sup> Fanpage called “Conflicts and World News”, about 22 000 followers, [on-line:] <https://www.facebook.com/Konflikty-i-Wiadomości-Światowe-103435204551498> (1.09.2022).

<sup>10</sup> Fanpage called “Conflicts and World News”, about 22 000 followers, <https://www.facebook.com/groups/548662952698344> (1.09.2022).

and Ukrainians (the first name of the group was “We do not believe in the Covid-19 pandemic” – changed on the 18th of March 2022). In addition to social networks, disinformation and propaganda content was introduced to the Polish infosphere via alternative portals (Sputnik was also involved in this activity until February 2022).

Portals such as “Niezależny Dziennik Polityczny” [“Independent Political Journal”], ‘Neon24.pl’ or “Najwyższy Czas” [“High Time”] (which may seem to have restricted the broadcasting of content openly coinciding with Russian propaganda after 2022) can be considered as examples of active sources that disseminate theses converging with Russian propaganda. Each of the listed ones has its own characteristics. The first is a source of primitive messages and fake news, which particularly relate to stimulating anti-American, anti-Ukrainian and anti-government sentiments. The latter is a platform that disseminates conspiracy theories, extremely anti-Ukrainian messages and materials published on the pages of other similar websites, strengthening the reach of several sources distributing content consistent with Russian propaganda (including the publication of “NDP”).<sup>11</sup> The third of these is a source that distributes conspiracy theorist content (e.g., questioning the existence of the pandemic)<sup>12</sup> or anti-Ukrainian content.<sup>13</sup> It is worth noting that the publications of these websites are actively popularised on social networks on groups and fanpages that publish disinformation content regarding conspiracy theories, geopolitics, foreign policy or internal policy. In addition to groups, fanpages and alternative portals, propaganda and disinformation content is being distributed online by sources posing as news and opinion portals.

In addition to Russian, the indicated sources of content are similar to Russian messages, they are published by sources such as “Konserwatyzm” [“Conservatism”] or “Myśl Polska” [“The Polish Thought”]. It is worth noting that both the indicated portals and the aforementioned “NDP” have often become sources of propaganda messages that the Russian side used for its own information market (their publications were often used for legitimising Russian-language messages propaganda). “Conservatism” and “The Polish Thought”, as opposed to “NDP” or “High Time”, are created as “serious” sources that avoid conspiracy theories and focusing on the allegedly independent

---

<sup>11</sup> “ROSJA vs NATO, jak to jest? Bander junta znowu bez problemu morduje!!!”, *Neon24.pl*, 13.09.2022 [on-line:] <https://fakty-kontra-news.neon24.info/post/169263.rosja-vs-nato-jak-to-jest-bander-junta-znowu-bez-problemu-morduje> (1.10.2022).

<sup>12</sup> “Covidiańska wersja świata. Obowiązek szprycowania dla uczniów od 12 lat wzwyż. ‘Bo szczepionki działają’”, *Nczas*, 2.10.2021 [on-line:] <https://nczas.com/2021/10/02/covidianska-wersja-swiatego-owobiazek-szprycowania-dla-uczniow-od-12-lat-wzwyz-bo-szczepionki-dzialaja/> (1.09.2022).

<sup>13</sup> “Szok! Ukraina kryjówką dla dowódców Państwa Islamskiego? SBU właśnie zatrzymała jednego z nich”, *Nczas.com*, 18.11.2019 [on-line:] <https://nczas.com/2019/11/18/szok-ukraina-kryjowka-dla-dowodcow-panstwa-islamskiego-sbu-wlasnie-zatrzymala-jednego-z-nich/> (1.09.2022).

description of the reality in the field of Polish domestic politics and international politics. Both “Conservatism” and “The Polish Thought” persistently publish material that stimulates anti-Ukrainian, anti-NATO and anti-EU attitudes. These sources also introduce to the Polish infosphere messages relating to the socio-political situation in Ukraine – which coincide with Russian propaganda theses that disinform Polish recipients about the current situation in Ukraine.

The materials published in the discussed sources lobby messages about Ukraine’s responsibility for the suffering of the Donbas population by depicting the Armed Forces of Ukraine as the “Nazi” structure,<sup>14</sup> messages portraying NATO as a weak, unnecessary – or even harmful – structure<sup>15</sup> or materials undermining the trust of the population in Polish services and institutions of the Polish state.<sup>16</sup> Some of the sources mentioned above and the like also operate via the YouTube platform, broadcasting recordings that duplicate disinformation and propaganda messages. There is also a noticeable tendency in which these and similar groups try to build a Polish-language segment of Telegram.

Analysing the material published by sources identified as releasing content similar to Russian propaganda (groups and fanpages operating on social networks, alternative portals, portals imitating serious news sources and channels using on YouTube), we can point to the leading directions in the development of Russian propaganda messages addressed to the Polish audience. The focus of centres distributing communications similar to Russian propaganda indirectly indicates the goals Russia is trying to achieve in Poland.

Leading trends:

- stimulating anti-government moods (undermining trust in state institutions, depreciating the image of the ruling class);
- stimulating anti-American and anti-NATO sentiments (messages most often concern both issues in parallel);
- stimulating anti-Ukrainian moods;
- stimulating Euroscepticism.

These trends are most often developed in such a way as to undermine the sense of the pro-Western/pro-EU attitude of the dominant part of the Polish political elite.

<sup>14</sup> S. Pikta, “Nadzieja i smutek na Donbasie (część 2)”, *Mysł Polska*, 2.11.2021, [on-line:] <https://myslpolska.info/2021/11/02/nadzieja-i-smutek-na-donbasie-czesc-2/> (1.09.2022).

<sup>15</sup> S. Lewicki, “Czy NATO jeszcze istnieje?”, *Konserwatyzm.pl*, 10.11.2019 [on-line:] <https://konserwatyzm.pl/lewicki-czy-nato-jeszcze-istnieje/> (1.09.2022).

<sup>16</sup> M. Piskorski, “PISM czy PiSM? Analitycy czy propagandziści?”, *Mysł Polska*, 4.11.2021 [on-line:] <https://myslpolska.info/2021/11/04/pism-czy-pism-analitycy-czy-propagandzisci/> (1.09.2022).

Anti-American, anti-NATO, anti-EU and anti-Ukrainian contents are shaped in such a way as to prove the harmfulness of the current political line.

The Russian side seems to notice the low effectiveness of the methods used until 2021 – hence the attempts to acquire new tools to influence Polish society. One of the tools that the Russian side is trying to use against Poland is Telegram. Until recently (mid-2021), it seemed that Telegram would remain an almost unknown platform in Poland that would not impact Polish society.

As of the beginning of 2022, Telegram still does not have an extensive Polish-language segment. However, new channels are emerging that are not only linked to circles openly cooperating with the Russian side, but entirely new anonymous channels are also being noticed. They disseminate, among others, materials published by the State Border Committee of Belarus in connection with the migration crisis and try to popularise [in Poland] narratives about the responsibility of the Polish services for the alleged “genocide” of migrants. The content of entries emitted by given channels often contains inflectional errors and mistakes resulting from the translation of the text from the Russian language. The Russian side will likely make efforts to continue the discussed process aimed at acquiring a new tool of influence on Polish society.

## Directions of the narrative

At this point, it is worth elaborating on the question of the directions indicated at the beginning of the study concerning the development of messages and narratives. One of them is stimulating anti-government sentiment in an attacked country. These activities aim to cause political chaos to destabilise the socio-political situation. On the one hand, these activities may concern attempts to cause chronic political chaos in a given country (which will limit, for example, the country’s defence capabilities) and, on the other, may focus on replacing a given government with an environment more favourable to Moscow. Activity in this area is most often combined with the fields of study that will be mentioned next or concerns current affairs that can serve to stimulate the polarisation of society. One such “current issue” is the Covid-19 matter. This issue could potentially build a split in society based on the population’s attitude to vaccination or the pandemic itself. In this context, the Russian side has taken actions in the field of disinformation in the Polish orientation, trying to build a negative image of Western vaccines while simultaneously stimulating a positive image of

the “Sputnik V” vaccine.<sup>17</sup> Relevant publications lobbying this narrative appeared in pages of the “Polish” editorial board of Sputnik and manifested themselves on portals identified as involved in the distribution of messages in line with Russian propaganda. Sputnik and the portals in question are engaged in parallel in publicising the protests of supporters of the conspiracy theses, portraying the pandemic as a “conspiracy” and denying the sense of vaccination.<sup>18</sup> This kind of activity, carried out by Russian-language media and through groups on the social network Facebook, has manifested itself in a particular way in Lithuania. For the Russian side, the Covid-19 pandemic became another factor included in efforts to destabilise the situation in the country by stimulating anti-government sentiment based on the pandemic.<sup>19</sup>

The direction concerning the stimulation of anti-government moods, developed in the countries of NATO’s so-called “eastern flank” and in Ukraine, repeatedly refers to a process serving to stir up anti-NATO and anti-US sentiment. In Poland, propaganda centres imitating Polish sources focus on this orientation. The portal “NDP” shows exceptional activity in this field – creating, among others, audio-visual materials made available on YouTube and on social networks. These materials often raise the issue of the risk of war (destruction of Poland) – the spectre of which is to be drawn over the country by the presence of US and NATO troops. A serious amount of attention paid by this and similar circles (mentioned in the text) relates to the risk of a nuclear attack that may occur as a result of the completion of the project to build a component of the US Aegis Ashore anti-missile system (in Redzikowo). The theme of attempts to depreciate the image of American soldiers based on the distribution of “fake news” and manipulated messages about alleged fights and the murder of the local population by American soldiers is also often manifested. In this context, there are also messages exposing rare cases of road collisions involving US soldiers. The aim of these activities is to build an image of the threat posed to Poles and the Polish state by the presence of American troops in the country and the military alliance with that state itself.

The third of the constant fields of influence of the Russian Federation relates to stimulating anti-Ukrainian moods in Poland. For this purpose, chronic activities are

---

<sup>17</sup> “Węgry: Sputnik V jest bardziej skuteczny niż pięć innych szczepionek”, *Sputnik Polska*, 25.11.2021, [on-line:] <https://pl.sputniknews.com/20211125/wegry-sputnik-v-jest-bardziej-skuteczny-niz-piec-innych-szczepionek-16624979.html> (1.09.2022).

<sup>18</sup> “Stop koronaścienie, stop przymusowi szczepień: protestujący chcą dymisji rządu”, *Sputnik Polska*, 22.02.2022, [on-line:] <https://pl.sputniknews.com/20210220/stop-koronascienie-stop-przymusowi-szczepien-protestujacy-chca-dymisji-rzadu-13865433.html> (1.09.2022).

<sup>19</sup> R. Richard, A.L. Pieciukaitis, *Moscow’s Disinformation Offensive During COVID-19: The Case of Lithuania*, Hudson Institute, 2020.

carried out (intensified depending on the international situation) aimed at presenting Ukraine and Ukrainians as a threat to the lives of average Poles and as a factor detrimental to the interests of Poland. Leading examples of the influence of Russia in 2021 were the popularisation of information messages about fights with the participation of Ukrainian citizens. Single examples of acts of violence (physical or verbal) are displayed on purpose, thus creating an impression of the massiveness of a given phenomenon – which differs from the actual state. The aim of the Russians was to create an image of a Ukrainian as a troublemaker/hooligan/alcoholic associated with activities aimed at depreciating the image of the Ukrainian state – a defective country with which cooperation is pointless. Based on these combined narratives, the Russian side tried to establish a belief that projects aimed at increasing the level of cooperation between Poland and Ukraine (including the Lublin Triangle) were pointless or harmful. In parallel to the proliferation on social networks and alternative portals of messages portraying an extremely negative image of Ukrainians, provocative operations were developed in Polish-Ukrainian relations. Examples of such action is the vandalism in Krakow in November 2021, when the monument to Marshal Józef Piłsudski and the Legion Four was damaged.<sup>20</sup> This attack was clearly an attempt to make it look like the activity of “Ukrainian nationalists”. The illogical slogans used at that time (“Poland not only for masters”) and errors (including the simultaneous use of the Russian and Ukrainian notation) clearly resembled the earlier provocations that took place, among others, in Kharkiv in March and July 2019 (the destruction of the UPA memorial plaque simulating an attack by Poles) or the 2017 act of vandalism that took place in Bykivnia near Kyiv (the Polish and Ukrainian part of the memorial dedicated to the victims of communist crimes was destroyed on the same night). In the context of the provocation in Krakow, it is also worth mentioning the hacking attack on Ukrainian government portals that took place from the 13th of January to the 14th of January, 2022. As part of the attack, the party responsible for a given operation placed a graphic with Ukrainian, Russian and Polish text suggesting that the attack was the responsibility of the Polish side (the content of the Polish-language entry – original version [with mistakes]: “Ukrainians! All your personal data has been sent to the shared network. All data on the computer is destroyed. It cannot be recovered. All information about

---

<sup>20</sup> “Akt wandalizmu w Krakowie. Nieznani sprawcy zniszczyli pomnik Piłsudskiego”, *Onet.pl*, 6.11.2021, [on-line:] <https://wiadomosci.onet.pl/krakow/krakow-akt-wandalizmu-nieznani-sprawcy-zniszczyli-pomnik-pilsudskiego/qvw2rdz> (1.09.2022).

you has become public, fear and wait for the worst. It's for you for your past, present and future. For Wołyń, for the OUN UPA, Galicia, Polesie and for historical areas").<sup>21</sup>

All of the examples mentioned above of provocation, by their nature and potential targets, point to the Russian Federation as the party behind the organisation or procuring of the activities in question. However, the provocative actions indicated do not seem to bring the results desired by the Russian Federation. The above-mentioned activities did not affect a wider circle of public opinion in Poland and Ukraine, as evidenced by the scale of the aid provided to Ukrainian refugees after February 2022. The indicated actions only seemed to reinforce anti-Ukrainian sentiments among radical pro-Russian groups whose representatives are strongly influenced by Russian disinformation centres. Thus, one can get the impression that the actions of the Russian Federation with the use of radical measures (e.g., indicated provocations) only served to maintain the level of anti-Ukrainian sentiment among the marginal group of people under the influence of the Kremlin (maintaining the influence already held – a similar process applies to stimulating anti-American sentiment through alternative websites). This trend changed significantly after February 2022, when the Russian side – through its centres of influence – decided to focus on stimulating anti-Ukrainian moods to cause social unrest, which would result in the suspension of military, economic and political support from Warsaw to Kyiv.

The fourth major field in developing Russian communications is stimulating Eurosceptic sentiments. As part of this aspect of disinformation and propaganda efforts, Russians can count on the activities of pro-Russian portals and circles, which – unlike the “NDP” – have “real” (not anonymous) editors and individuals who seek to participate in the socio-political life of the state. This direction is also developed based on anonymous sources (operating on social networks or in “created editorial offices” as “imaginary journalists”). As part of the information activity on stimulating Eurosceptic moods, narratives are developed that are manifested in almost all EU countries. They refer to the building of an image of the EU as a structure hostile to national identity, Christian culture, tradition, prevailing moral norms in the country, etc. The EU is also portrayed as a structure fully controlled by Germany, which – in Polish conditions – is combined with propaganda activity aimed at stimulating anti-German sentiment. In this context, the EU is to be an instrument of Berlin’s “imperial” policy, which threatens Polish statehood. To build narratives that are appropriate from the Kremlin’s perspec-

---

<sup>21</sup> M. Marek, “Atak na ukraińskie portale rządowe – próba zrzucenia odpowiedzialności na Polaków”, *Centum Badań Nad Współczesnym Środowiskiem Bezpieczeństwa*, 14.01.2022 [on-line:] <https://infowarfare.pl/2022/01/14/atak-na-ukrainskie-portale-rzadowe/> (1.09.2022).

tive, political and media “authorities” who are “friendly” to the Russian Federation are again being used. This is in addition to individuals who are far from cooperating with the Kremlin but who support the development of Eurosceptic sentiment for other reasons. Their comments are also used to reinforce Russian narratives (the most radical statements are deliberately selected and then properly displayed – e.g., in headlines). The Eurosceptic direction of activity is associated with the stimulation of anti-German, anti-American and anti-NATO moods. The formed narratives fit into the context of creating the image of Poland’s subordination to the West (in any form, be it NATO or the EU). At the same time, the pro-Western political elite of Poland is being portrayed as “puppets” of the West, which must be “pushed away” from power and replaced with “truly Polish” forces (e.g., those postulating “normalisation” of relations with Russia and the rejection of “subjection” to the USA and the EU). The development of communications in all of the directions mentioned above boils down, *de facto*, to influencing the political preferences of Poles to maintain and expand the network of audiences who, when the time comes, will be able to be a factor influencing the political scene of the Polish state.

## Summary

Currently, the Russian side has a limited influence on Polish society. However, there are visible actions in the form of attempts to acquire new tools and techniques (e.g., anonymous comments published on a mass scale under articles from popular Polish internet portals), enabling the Kremlin to influence an ever wider group of Poles. Depending on the international situation, the Russian part adjusts its activities to its priorities. In the case of 2021, there was intensification of the activity in the field of Polish-Russian-Belarusian relations, which was the result of the crisis on the Polish-Belarusian border. The year 2022, however, indicates that Polish-Ukrainian relations (the context of the ongoing war in Ukraine) are considered one of the current priorities. The Russian side is trying to use each of the convenient trends to stimulate social discontent among Poles and direct it towards pro-Western/pro-Ukrainian political elites and towards a dislike of Ukrainian refugees (including the issue of the raw material crisis, which has intensified in the second half of 2022).

The main task facing NATO’s so-called “eastern flank” is long-term work with its own society to increase social resilience to disinformation. New information campaigns and media projects are needed to reach the so-called “average recipient” and will offer them interesting materials making them aware of the scale of information threats.

Work with citizens must be supplemented with popularising knowledge in a given area among decision-makers. It remains important not to forget about information security when implementing projects relating to increasing awareness of cyber threats. The activity of the Russian Federation (relating to the stimulation of tensions between NATO member states and Western-backed Ukraine in the defence war) should also be counteracted through active expert cooperation aimed at producing analyses and journalistic materials that are attractive to the public and that deconstruct historical myths (e.g., created during the USSR period) and false stereotypes about the countries in question. It is also worth developing cooperation between the countries of NATO's eastern flank and Ukraine in the field of acquiring capabilities allowing information operations dedicated to Russian-speaking recipients living in the post-Soviet spaces.

## References

- “Akt wandalizmu w Krakowie. Nieznani sprawcy zniszczyli pomnik Piłsudskiego”, *Onet.pl*, 6.11.2021, [on-line:] <https://wiadomosci.onet.pl/krakow/krakow-akt-wandalizmu-nieznani-sprawcy-zniszczyli-pomnik-pilsudskiego/qvw2rdz>.
- “Covidiańska wersja świata. Obowiązek szprycowania dla uczniów od 12 lat wzwyż. ‘Bo szczepionki działają’”, *Nczas*, 2.10.2021 [on-line:] <https://nczas.com/2021/10/02/covidianska-wersja-swiata-obowiazek-szprycowania-dla-uczniow-od-12-lat-wzwyz-bo-szczepionki-dzialaja/>.
- “Kursk’ o wydaniu ‘Mein Kampf’ w Polsce: Propagowanie totalitaryzmu”, *Sputnik Polska*, 20.01.2021, [on-line:] <https://pl.sputniknews.com/20210120/mein-kampf-po-polsku-kursk-kieruje-sprawe-do-prokuratury-sputnik-13700194.html>.
- Lewicki S., “Czy NATO jeszcze istnieje?”, *Konserwatyzm.pl*, 10.11.2019 [on-line:] <https://konserwatyzm.pl/lewicki-czy-nato-jeszcze-istnieje/>.
- Magda Ê., *Gibridna agresia Rosii: Uroki dla Êwropi*, Kalmar, Kiïv 2017 [Магда Є., *Гібридна агресія Росії: Уроки для Європи*, Калмар, Киïв 2017].
- Marek M., “Atak na ukraińskie portale rządowe – próba zrzućenia odpowiedzialności na Polaków”, *Centum Badań Nad Współczesnym Środowiskiem Bezpieczeństwa*, 14.01.2022 [on-line:] <https://infowarfare.pl/2022/01/14/atak-na-ukrainskie-portale-rzadowe/>.
- Marek M., “Białoruski’ ślad w operacji dot. ataku na skrzynkę M. Dworczyka – analiza działalności ośrodka propagandowego ‘Belvpo’”, *Centum Badań Nad Współczesnym Środowiskiem Bezpieczeństwa*, 5.07.2021 [on-line:] <https://infowarfare.pl/2021/07/05/bialoruski-slad-w-operacji-dot-ataku-na-skrzynke-m-dworczyka/>.
- Marek M., “Bieżąca aktywność ośrodków medialnych lobbujących w Polsce rosyjski przekaz dezinformacyjny – konsolidacja środowiska trwa”, *Centum Badań Nad Współczesnym Środowiskiem Bezpieczeństwa*, 21.07.2021 [on-line:] <https://infowarfare.pl/2022/07/21/biezaca-aktywnosc-dezinfo-osrodkow-medialnych-konsolidacja-srodowiska/>.

- Pikta S., "Nadzieja i smutek na Donbasie (część 2)", *Mysł Polska*, 2.11.2021 [on-line:] <https://myslpolska.info/2021/11/02/nadzieja-i-smutek-na-donbasie-czesc-2/>.
- Piskorski M., „PISM czy PiSM? Analitycy czy propagandziści?”, *Mysł Polska*, 4.11.2021 [on-li] <https://myslpolska.info/2021/11/04/pism-czy-pism-analitycy-czy-propagandzisci/>.
- Richard R., Pieciukaitis A.L., *Moscow's Disinformation Offensive During COVID-19: The Case of Lithuania*, Hudson Institute, 2020.
- “Rekordowa liczba imigrantów zarobkowych w Polsce. Niezaspokojony popyt”, *Rzeczpospolita*, 25.01.2022 [on-line:] <https://www.rp.pl/rynek-pracy/art19323661-rekordowa-liczba-imigrantow-zarobkowych-w-polsce-niezaspokojony-popyt>.
- “ROSJA vs NATO, jak to jest? Bander junta znowu bez problemu morduje!!!”, *Neon24.pl*, 13.09.2022 [on-line:] <https://fakty-kontra-news.neon24.info/post/169263,rosja-vs-nato-jak-to-jest-bander-junta-znowu-bez-problemu-morduje>.
- “Stop koronaścienie, ‘stop przymusowi szczepień’: protestujący chcą dymisji rządu”, *Sputnik Polska*, 22.10.2022 [on-line:] <https://pl.sputniknews.com/20210220/stop-koronascienie-stop-przymusowi-szczepien-protestujacy-chca-dymisji-rzadu-13865433.html>.
- “Szok! Ukraina kryjówką dla dowódców Państwa Islamskiego? SBU właśnie zatrzymała jednego z nich”, *Nczas.com*, 18.11.2019 [on-line:] <https://nczas.com/2019/11/18/szok-ukraina-kryjowka-dla-dowodcow-panstwa-islamskiego-sbu-wlasnie-zatrzymala-jednego-z-nich/>.
- Trzebiński J., *Narracja jako sposób rozumienia świata*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 2002.
- “Węgry: Sputnik V jest bardziej skuteczny niż pięć innych szczepionek”, *Sputnik Polska*, 25.11.2021, [on-line:] <https://pl.sputniknews.com/20211125/wegry-sputnik-v-jest-bardziej-skuteczny-niz-piec-innych-szczepionek-16624979.html>.
- Wojnowski M., “‘Zarządzanie refleksyjne’ jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.”, *Przegląd Bezpieczeństwa Wewnętrznego*, vol. 7 (2015).



# The Russia-Ukraine War Two Strategies of Communication?

**ABSTRACT:** In the aftermath of the Russian invasion of Ukraine, reflections on the communication strategies and tactics used to perform tasks that form part of an information war have again become a topical question. The objective of this paper is, therefore, to analyse the strategic communication practices used during the Russia-Ukraine war. It also attempts to examine the wartime effectiveness of using such forms of communication as propaganda, disinformation, or fake news, as well as techniques used to uncover the false information being spread. The article formulates the following research hypotheses: H1. The Russia-Ukraine war is an example of a new approach to information war. H2. Both sides of the Russian-Ukrainian conflict use different communication strategies. H3. The information war waged during the Russian-Ukrainian conflict is a method of pursuing military, political and economic goals.

**KEYWORDS:** propaganda, disinformation, communication

## Introduction

In the aftermath of the Russian invasion of Ukraine, reflections on the communication strategies and tactics used to perform tasks that form part of an information war have

again become a topical question. The objective of this paper is, therefore, to analyse the strategic communication practices used during the Russia-Ukraine war. It also attempts to examine the wartime effectiveness of using such forms of communication as propaganda, disinformation or fake news, as well as techniques used to uncover the false information being spread.

Using disinformation as a component that complements military action is not a new solution, but the development of the internet – in particular, social media – enabled and improved this form of communication, which allowed public opinion, an important actor in political communication, to be influenced in an even better and easier way. The article formulates the following research hypotheses: H1. The Russia-Ukraine war is an example of a new approach to information war; H2. Both sides of the Russian-Ukrainian conflict use different communication strategies; H3. The information war waged during the Russian-Ukrainian conflict is a method of pursuing military, political and economic goals.

## Information war – an evolution of the concept

The information revolution (i.e., all processes related to the increasing level of digitisation and technologisation of our everyday lives) has not been without impact on other important issues related to the social, political or crisis communication process or strategies used during armed hostilities. The same applies to the concept of “information war”, which started to appear in the early 1990s in both official reports and specialised literature, together with other concepts such as “information domination”, “infowar”, “cyberwar” and “cognitive war”. None of these terms has been clearly defined, and we can agree with Hervé Coutau-Bégarie, who stated that the “trend for information war is accompanied by a significant vagueness of its specific content”.<sup>1</sup> However, we can assume that information war is a continuation of electronic war, which has been known for decades.<sup>2</sup> Some researchers believe that the essential nature of information war boils down to physical action, where “information has a strategic value and deserves to be conquered and destroyed”,<sup>3</sup> which can, for example, mean attacks on the critical infrastructure of a given country.

---

<sup>1</sup> H. Coutau-Bégarie, *Traité de stratégie*, Economica, Paris 1999, p. 271.

<sup>2</sup> S. Czeszejko, J. Janczak, “Militarne aspekty środowiska elektronicznego – próba rewizji istniejącej terminologii”, *Zeszyty Naukowe AON*, vol. 1, no. 98 (2015), pp. 78–81.

<sup>3</sup> W. Schwartau, *Information Warfare: Protecting Your Personal Security in the Computer Age*, Thunder’s Mouth Press, New York–Emeryville, CA 1996, p. 317.

This is the situation we have been witnessing ever since Russia's aggression on Ukraine. Microsoft has shown that when the coalition of countries supporting Ukraine was created, Russian attacks against the governments of these states significantly intensified – analysts detected attempts to hack 128 organisations in 42 countries, including Poland, although the US remains the main target of attacks. It is estimated that around 29% of these attacks were successful. Attacks were most frequently aimed at government agencies, IT companies and institutions responsible for administering critical infrastructure systems – all key for ensuring the continuous operation of the state.<sup>4</sup> We must remember that cyberattacks on railway companies, medical centres, banks, waterworks or powerplants can be very damaging. Their consequences may paralyse the operations of the attacked state and cause huge economic and financial losses, or even deaths.

Of note is the fact that Russia carried out multiple attacks on Ukrainian computer networks in recent months.<sup>5</sup> The resources and digital infrastructure of the Ukrainian government and institutions survived only thanks to being quickly transferred to the public cloud and located in data centres dispersed around Europe.

There is another equally important dimension to information war, namely the psychological dimension. The concept of psychological war reappeared in the 1990s due to the Balkan conflict. Psychological war usually involves operations aimed at attacking the enemy's morale or beliefs, its leaders, its population and its allies, but also protecting a country's population, leaders and allies against actions taken by the opponent as part of psychological war. We can point here to the "Voice of America" or "Radio Free Europe" as very effective tools in the information war during the Cold War.

## Methods of waging information war by the Russian Federation

There can be no doubt that psychological warfare is part of information wars waged by the Russian Federation, which also uses so-called "soft power", is seen by some researchers to play an ever-increasing role in shaping the image of the Russian state

---

<sup>4</sup> B. Smith, "Defending Ukraine: Early Lessons from the Cyber War", *Microsoft*, 22.06.2022, [on-line:] <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/> (12.08.2022).

<sup>5</sup> "Cyberataki hakerów z Rosji na ukraińskie sieci komputerowe. Przejęli wrażliwe dane", *Polsat News*, 16.02.2022, [on-line:] <https://www.polsatnews.pl/wiadomosc/2022-02-16/cyberataki-hakerow-z-rosji-na-ukrainskie-sieci-komputerowe-przejeci-wrazliwe-dane/> (12.08.2022).

in the international arena.<sup>6</sup> The war is, therefore, waged both internally and externally as its goal, on the one hand, is to influence Russian citizens and, on the other, to gain the trust of some of the world's leaders and international public opinion [with them].<sup>7</sup>

Russian psychological warfare is, therefore, not limited to using black propaganda, but is more sophisticated and combines lies, slander, insinuations and “partial truth”. Its main objective can be to deprive its audience of any references and evidence, and it usually misrepresents important historical events.<sup>8</sup> In the external dimension, the strategy is pursued using multiple avenues, with one of the most well-known being the propaganda disseminated by the so-called “troll army” on social media, primarily on Twitter and Facebook.<sup>9</sup> Their task is not only to attack and criticise their opponents, but also to impose false narration on the audience, often using aggressive, even racist or antisemitic rhetoric. “Post-truth” is, therefore, their favoured tool, accompanied by the ever-present criticism of “mainstream media”. Russian propaganda is also pushed by official channels of the Kremlin, such as *Russia Today*<sup>10</sup> and *Sputnik*,<sup>11</sup> who broadcast and tweet in many languages. These channels not only echo the Kremlin's agenda (including the claims suggesting that there are no Russian troops in Ukraine, pushed even before the attack on Ukraine, or the assertions that the Russian forces were not attacking insurgents fighting Assad's regime, etc.), but also try to reach all potential Putin sympathisers and find new ones. The fact that the Russian regime supports politicians from various parties, although primarily those on the right side of the political spectrum, both in Europe and in the US, is also important. Proof of this

---

<sup>6</sup> D. Kaźmierczak, “Walka informacyjna we współczesnych konfliktach i jej społeczne konsekwencje”, *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate et Educatione Civili*, vol. 7 (2017).

<sup>7</sup> O. Irisova, “A Lie is the Truth, Intersection Project”, *Intersection Project*, 3.07.2015, [on-line:] <http://intersectionproject.eu/article/society/lie-truth> (27.09.2022).

<sup>8</sup> A. Foxall, “In Putin's Russia, History Is Subversive”, *The American Interest*, 6.06.2016, [on-line:] <https://www.the-american-interest.com/2016/06/06/in-putins-russia-history-is-subversive> (9.08.2022).

<sup>9</sup> T. Parfitt, “My Life as a pro-Putin Propagandist in Russia's Secret Troll Factory”, *The Telegraph*, 24.06.2015, [on-line:] <https://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/MyLife%20as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory/> (9.08.2022).

<sup>10</sup> RT – a TV news station founded by the Russian government on December 10, 2005, based in Moscow, broadcasting 24 hours a day, 7 days a week.

<sup>11</sup> Sputnik – Russian government news agency launched on November 10, 2014 by Rossiya Siewodnia, which has a network of radio stations and multilingual websites. Its regional offices are located in many countries, including United States (Washington, DC), China (Beijing), France (Paris), Germany (Berlin), Egypt (Cairo) and Great Britain (London and Edinburgh).

fact could be seen in the presidential campaigns in the US and France, and Russia's support for proponents of Brexit.<sup>12</sup>

Information war waged in this way involves both offensive and defensive action. Its current version is related to the Russian Federation's war doctrine, announced in December 2014. The concept harks back to Soviet methods based on using "psychological warfare" and propaganda techniques used back in the times of the USSR. However, tools used in information wars were improved due to events which were not always proof of the effectiveness of Russian military strategy and tactics. The first important event of this kind occurred in 1999, when Russian decision-makers noticed (during the war in Chechnya) that Chechen soldiers were much more proficient in using the internet and were able to reach a global audience with their message by presenting themselves as "heroic fighters for the freedom of Chechnya fighting against the Russian war machine".<sup>13</sup> It was then that the Russians noticed that the internet could be a tool used for destabilisation or even as a threat to national security. Due to this, a decision was made that public access to the internet must be effectively controlled. The Kremlin also became aware that digital technologies can be used to attack enemies, both internal and external. Another significant event took place during the short military conflict with Georgia in 2008, when Russian decision-makers noticed how the then Georgian President, Mikhail Saakashvili, had no problems reaching an audience in the West by giving speeches in English. This was in contrast to Russian media campaigns, which were based on frequently belated and poorly prepared press conferences.<sup>14</sup>

This Georgian lesson gave birth to the idea of creating solutions involving experts in strategic communications, diplomats, military men, journalists or even hackers, who would use their abilities to wage effective psychological operations as part of the ongoing information war. The last event which further convinced Russia that the web and social media must be controlled was the "Arab Spring". Russian authorities decided that automated systems alone were insufficient and significant human resources had to be allocated to control the internet. Some important personnel changes also took place in that period: Vyacheslav Volodin replaced Vladislav Surkov as the Deputy Director

---

<sup>12</sup> A. Kruglashov, S. Shvydiuk, "Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory", *Wschód Europy. Studia Humanistyczno-społeczne*, vol. 6, no. 2 (2020), pp. 79–92.

<sup>13</sup> M. Maciejak, *Anatomia konfliktu rosyjsko-czeczeńskiego. Grozny 1994/1995, 1999/2000*, Infortedionis, Zabrze 2018, p. 401.

<sup>14</sup> R. Grodzki, *Wojna gruzińsko-rosyjska 2008: przyczyny, przebieg, skutki*, Wydawnictwo Replika, Zakrzewo 2009, p. 137.

of the Presidential Administration and was tasked with preparing and implementing a new Russian communication strategy based on the tenets of information war. In addition, in November 2012, Sergei Shoigu replaced Anatoly Serdyukov as the Minister of Defence of the Russian Federation. One of the major tasks given to the new Minister was to work on improving guidelines related to Russian cyberstrategy. The document, published on December 29, 2014 on the website of the Council of Defence of the Russian Federation, contains a statement that “information is an important tool of security”.<sup>15</sup> Although the concept wasn’t novel (as the military doctrine and information security doctrine of 2000 included the same statement), it was only in the document from 2014 that the following passage was included: “the main external war threat involves the use of information and communication technology for military and political goals and engaging in actions contrary to international law, aimed against the sovereignty, political independence, territorial integrity (...)”. In addition, another passage stated that the “Russian information war constitutes the entirety of various actions coordinated in time, performed by the military and civil intelligence services in many areas, in order to neutralise the enemy using information and technical and information and psychological tools”<sup>16</sup>. Other information threats include dangers such as encouraging young people to leave behind their historical, spiritual and patriotic traditions, as well as destruction or at least disruption of operations of governmental agencies or state information infrastructure. Another new rule is the underlining of the statement that the line between internal and external threats is becoming blurred and that Western information technologies are downright “subversive”.

It, therefore, did not come as a surprise that on February 24, 2022, the Russian Federation not only commenced another stage of its military operation in Ukraine, but also continued its information war, including in terms of its image. The hostilities involve all forms and tools available to both sides for wartime communication, including propaganda, which – according to Jacques Ellul, one of the major theoreticians of this phenomenon – “is important and present during all wars”.<sup>17</sup>

Both old and new media are, therefore, used in the Russian-Ukrainian war waged on many fronts, including in the information war. They are primarily used not for providing information, but as tools of persuasion and propaganda. In its communication strategy, Russia primarily attempts to legitimise its attack on Ukraine while simultaneously presenting Ukraine not as a victim, but as a provocateur and cause for

---

<sup>15</sup> “Doktryna Wojenna Federacji Rosyjskiej”, *bbn.gov.pl*, [on-line:] <https://www.bbn.gov.pl/ftp/dok/01/DoktrynaFederacjiRosyjskiej.pdf>, pp. 6–8 (25.09.2022).

<sup>16</sup> *Ibidem*.

<sup>17</sup> J. Ellul, *Propaganda: The Formation of Men's Attitudes*, Alfred A. Knopf, New York 1973, p. 211.

the Russian intervention. On the other hand, Ukrainian authorities use any available forms and tools of communication to gain the support of international public opinion and leaders of democratic countries to promote their cause on a political level.

An important task in this regard is to build an adequate narrative – the purpose of which is not always to convey true and verified facts, but to fulfil an emotive role which involves presenting opinions aimed at creating the desired image of presented events.

As previously noted, the Russian Federation has gradually changed its approach to methods of communication, which includes noticing the important role played by “soft power” tools. Since the 2010s, the Kremlin has been increasingly interested in regaining control over the message pushed in audio-visual media and being aware of the power of digital technology it continually invested in social media so as to be able to “tell” its own version of events – the causes, course and outcome of various conflicts in which it was involved. An example of an investment in social media is the takeover of the VKontaktie (VK) Russian social media website – also known as the “Russian Facebook” – by oligarchs closely associated with Vladimir Putin (Alisher Usmanov and Igor Sechin). VK was founded in 2006 by Pavel Durov. Its structure and functionality are reminiscent of Facebook as its members can send messages, publish photos, videos and posts, and create groups. VK is among the most popular websites in Russia, Kazakhstan, Moldova, Kyrgyzstan, Uzbekistan, Armenia and Belarus. Many of its users are also citizens of Central and Eastern European countries.<sup>18</sup> Until 2017, it was also widely used in Ukraine but, pursuant to a decree of Petro Poroshenko – the then President of Ukraine – on May 16, 2017, some Russian websites were blocked, including VK and the Russia Today TV station.<sup>19</sup> The Kremlin-controlled VK was a very useful tool for Russia and was used to promote events such as the 2014 Winter Olympic Games in Sochi and build a positive image of the Russian Federation in the international arena.

Another component of information war after February 24, 2022, as an integral part of Russian military doctrine, was making Facebook and Instagram illegal in the territory of the Russian Federation, followed by imposing restrictions on Russian users of Twitter and then completely blocking the website. However, the most important decision was the adoption of an act that introduced penalties of up to 15 years’ im-

---

<sup>18</sup> “WKontaktie, największy serwis społecznościowy Rosji, trafił w ręce osób związanych z Putinem”, *Komputer Świat*, 6.12.2021, [on-line:] <https://www.komputerswiat.pl/aktualnosci/wydarzenia/wkontaktie-najwiekszy-serwis-spoiecznosciovoy-rosji-trafil-w-rece-osob-zwiazanych-z-7cnjx60> (12.08.2022).

<sup>19</sup> K. Puto, “Na Ukrainie zamknęli internet”, *Krytyka Polityczna*, 19.05.2017, [on-line:] <https://krytykapolityczna.pl/felietony/kaja-puto/na-ukrainie-zamkneli-internet/> (12.08.2022).

prisonment for journalists who disseminated information aimed at “discrediting” the Russian armed forces. Although decisions were made to censor independent media, primarily local ones, Russia’s state and governmental accounts are still active on Facebook, Twitter and YouTube, which have been blocked for ordinary citizens. On July 18, 2022, a Russian court fined Alphabet (Google’s parent company) \$387m for failing to comply with an order to delete content which Russia believed to be illegal. The company’s bank account had been seized back in May 2022, which according to the company’s announcement, prevented it from “continuing the operations of our Russian offices, including to maintain employment and pay salaries, pay our suppliers and contractors and comply with other financial obligations”<sup>20</sup>. Russian authorities did not block the website to be able to continue to use its streaming services as they can be used for Russian propaganda.

As the war in Ukraine escalated, American websites also took action aimed at limiting the influx of fake news released by Russian-controlled media. In its report published on April 7, 2022, Meta (Facebook’s parent company) announced that it had taken action against a group of hackers who had attempted to spread false information that Ukrainian troops had surrendered.<sup>21</sup>

Pursuant to Council Regulation (EU) 2022/350 of March 1, 2022, the EU’s Office of Electronic Communications also modified existing regulations. The new regulation prohibited the broadcasting (and other activities facilitating the broadcasting) of Russia Today and Sputnik. The Office stressed that the prohibition included distributing content using any means – including cable, satellite, IP-TV, websites and video-sharing applications, whether new or preinstalled. Stations affected by the prohibition included *RT – Russia Today English*, *RT – Russia Today UK*, *RT – Russia Today Germany*, *RT – Russia Today France*, *RT – Russia Today Spanish* and *Sputnik*.<sup>22</sup> When explaining the decision to block RT and Sputnik, the Chief of EU Diplomacy, Josep Borrell, stated that “systematic manipulation of information and disinformation by the Kremlin is used as an operational tool in their attack on Ukraine. It also constitutes

---

<sup>20</sup> “Google znów ukarany w Rosji. 387 mln dol. kary za nieusuwanie treści”, *Business Insider*, 18.07.2022, [on-line:] <https://businessinsider.com.pl/technologie/nowe-technologie/google-ukarany-w-rosji-387-mln-dol-kary-za-nieusuwanie-tresci/4s6wkz3> (15.08.2022).

<sup>21</sup> “Meta’s Adversarial Threat Report: First Quarter 2022”, *Meta*, 7.04.2022, [on-line:] <https://about.fb.com/news/2022/04/metas-adversarial-threat-report-q1-2022> (10.08.2022).

<sup>22</sup> *Rozporządzenie Rady (UE) 2022/350 z dnia 1 marca 2022 r. w sprawie zmiany rozporządzenia Rady (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*, [on-line:] <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022R0350&from=EN> (25.09.2022).

a direct threat to the public order and security in the EU”<sup>23</sup>. Sanctions will remain in place until Russia ends its aggression in Ukraine and ceases its disinformation and manipulation in respect of the EU and its member states.

Simultaneously, on March 5, 2022, at the request of the Prosecutor General of the Russian Federation, the ‘Wot Tak’ channel, a Russian-language website operated by Belsat TV and addressed to visitors from former Soviet republics, was blocked in Russia. Belsat TV is a TV channel that forms part of *Telewizja Polska SA*, which is co-financed by the Polish Ministry of Foreign Affairs and is broadcast in Belarussian and Russian, including in the territory of the former USSR.<sup>24</sup>

As always, history and historical memory remain an important tool in the communication strategy of the Russian Federation. Before the invasion of Ukraine, on February 21, 2021, President Putin gave an address in which he harked back to the past in order to legitimise the future attack on Ukraine. By acknowledging the independence and sovereignty of the Donetsk and Luhansk People’s Republics and announcing the commencement of a “special military operation”, he suggested that this would lead to the liberation of the Ukrainian people oppressed by a corrupt government that has been manipulated by the West. He also added that it has always been the West’s goal to spread its sphere of influence in the East, obviously at the cost of weakening Russia.<sup>25</sup>

This narrative was primarily aimed at Russian citizens but also those with pro-Russian sympathies. Other addresses given by Vladimir Putin hit similar notes, such as the address of April 21<sup>26</sup> or the address given on May 9, 2022, during the celebration of the anniversary of the end of World War II.<sup>27</sup> In his speeches, the Russian President used both grey and black propaganda, numerous times referring to the ethnic cleansing of Russians allegedly carried out by Ukrainians in the Donbas. He even made comparisons to “antisemitic pogroms organised by Nazis in Germany in the 1930s”. He also suggests that Ukraine intended to purchase nuclear weapons and improve biological

---

<sup>23</sup> “Russia Today i Sputnik blokowane w Europie. Tak Unia walczy z rosyjską propagandą”, *Business Insider*, 9.03.2022, [on-line:] <https://businessinsider.com.pl/biznes/russia-today-i-sputnik-blokowane-w-europie/p56dt93> (25.09.2022).

<sup>24</sup> “Bielsat TV z serwisem informacyjnym po ukraińsku, portal Wot Tak zablokowany w Rosji”, *Wirtualne Media*, 9.03.2022, [on-line:] <https://www.wirtualnemedi.pl/artykul/bielsat-informacje-wojna-w-ukrainie-rosja> (25.09.2022).

<sup>25</sup> “Wojna na Ukrainie? Orędzie Putina z 21.02.2022”, *YouTube*, [on-line:] <https://youtu.be/uN-85c2jeAtM> (25.09.2022).

<sup>26</sup> “Orędzie Putina: pochwały, obietnice i pogróżki”, *Ośrodek Studiów Wschodnich im. Marka Karpia*, 21.04.2021, [on-line:] <https://www.osw.waw.pl/pl/publikacje/analizy/2021-04-21/oredzie-putina-pochwały-obietnice-i-pogrozki> (25.09.2022).

<sup>27</sup> “Dzień Zwycięstwa 9 Maj 2022 r. Przemówienie Putina”, *YouTube*, [on-line:] <https://youtu.be/81IyVpv75o4> (25.09.2022).

weaponry, all this with the support of and contributions from the “Pentagon”. Even though such actions undermine Russia’s image in Western democracies, they can still mobilise that part of international public opinion which, for one reason or another, does not approve of the current world order and is very critical of Western democracies.<sup>28</sup> An example of this can be seen in the allegations made against “mainstream Western media”, which unfairly treats Syrians or Iraqis compared to Ukrainians.

## Methods of waging information war by Ukraine

The Russian effort in the information war is naturally met by a reaction from the Ukrainian side. Even a cursory examination of these efforts, in particular the choice of communication strategy, shows that the Ukrainians and, in particular, President Volodymyr Zelenskyy, have a certain advantage over their Russian opponent. It is obvious that Ukraine has been able to win over the majority of Western public opinion but, most of all, President Zelenskyy has had a profound effect on his own citizens. He became a true symbol of resistance, a personification of the fight for freedom and Ukrainians’ right of self-determination. His communication strategy includes a daily video selfie, regular speeches given before parliaments of the largest nations or major international organisations – both political and economic – but also cultural things, as well as close contact with European and global leaders.

Therefore, it must be said that Volodymyr Zelenskyy has been dealing very well with various forms of communication and is effective in using means of communication that are adequate for a time of war by simultaneously adapting them to today’s standards of political communication, which include an all-encompassing hypermediatisation. This seems an extraordinary achievement given the fact that prior to Russia’s attack on Ukraine, President Zelenskyy was not among the most recognisable and famous world leaders. He was known more for his previous career as an actor. From the very start of the conflict, he took on a role of a soldier ready to fight and intensify the spirit of resistance, calling on every man of conscription age to take up arms and defend their homeland against the aggressor.

When analysing the actions of the Ukrainian President, we can distinguish several objectives he achieves using his communication strategy. In the beginning, the most important task was to show both to Ukrainians and international public opinion that

---

<sup>28</sup> W. Sokała, “Przyjaciele Putina: Watykan i kto jeszcze”, *Microsoft*, 22.01.2022, [on-line:] <https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8413152,jakie-panstwa-popieraja-rosje-i-dlaczego-onz.html> (25.09.2022).

he would not leave his country to fend for itself in this difficult time. His tweet, stating: “I need ammunition, not a ride”<sup>29</sup> (in response to an offer of evacuation from the US President), reverberated around the world. Zelenskyy disregarded his personal safety and remained in the capital (which was being bombarded), acting as an example for his citizens and encouraging them to stay in the country and continue fighting in defence of the homeland.<sup>30</sup>

Choosing to communicate via social media also turned out to be the correct choice as the Russians were unable to cut Ukraine from contact with international public opinion or governments of other countries despite bombing radio and TV broadcast centres. Of note is also the request by Ukraine’s Minister of Digital Transformation, Mykhailo Fedorov, who used Twitter to ask Elon Musk for access to Starlink to help Ukrainians stay online during the Russian invasion. A few hours later, in response to Fedorov’s tweet, Elon Musk stated that Starlink was made available in Ukraine.<sup>31</sup>

Social media has, therefore, become an important method of communication for Ukrainians as well. They are used to communicate the most important news on military action but also enable interactions with citizens around the world. Another important challenge facing President Zelenskyy was communicating with the Russian Federation (both Russian decision-makers and military personnel), but also common Russian citizens – who he addressed many times and asked not to become involved in military action or suggested that they desert if compulsory mobilisation is announced.<sup>32</sup>

Another important function of messages sent by the Ukrainian President is to ensure that the West provides Ukraine with support, not only political and economic, but primarily military, by supplying all necessary to wage war – particularly arms and military equipment. Of note is that Zelenskyy was able to achieve this goal by addressing its communication not only to political decision-makers, but primarily to common citizens – the majority of who support the decisions of their authorities and approve of not only sending strictly military aid to Ukraine, but also imposing further sanctions on the Russian Federation. When analysing the numerous addresses made

<sup>29</sup> “Katarzyna Włodkowska”, *Twitter*, [on-line:] [https://twitter.com/k\\_wlodkowska/status/1497452572784824320?s=20&t=bI6TdOKqvCd3uDOxPEMwLg](https://twitter.com/k_wlodkowska/status/1497452572784824320?s=20&t=bI6TdOKqvCd3uDOxPEMwLg) (28.09.2022).

<sup>30</sup> “ZelenskyyUa”, *Twitter*, [on-line:] [https://twitter.com/ZelenskyyUa/status/1497450853380280320?s=20&t=FEJfWBjdXRL\\_gZLKioQg](https://twitter.com/ZelenskyyUa/status/1497450853380280320?s=20&t=FEJfWBjdXRL_gZLKioQg) (28.09.2022).

<sup>31</sup> “Elon Musk”, *Twitter*, [on-line:] [https://twitter.com/elonmusk/status/1497701484003213317?ref\\_src=twsrc^tfw|twcamp^tweetembed|twterm^1497701484003213317|twgr^96d348165aad556abbe2ad6b109dbb59de6aaa68|twcon^s1\\_c10&ref\\_url=https://www.computerworld.pl/news/Elon-Musk-udostepnia-Starlink-na-Ukrainie436628.html](https://twitter.com/elonmusk/status/1497701484003213317?ref_src=twsrc^tfw|twcamp^tweetembed|twterm^1497701484003213317|twgr^96d348165aad556abbe2ad6b109dbb59de6aaa68|twcon^s1_c10&ref_url=https://www.computerworld.pl/news/Elon-Musk-udostepnia-Starlink-na-Ukrainie436628.html) (28.09.2022).

<sup>32</sup> “Zelenskiy Official”, *Instagram*, [https://www.instagram.com/reel/Ch24ikEpmSJ/?utm\\_source=ig\\_web\\_copy\\_link](https://www.instagram.com/reel/Ch24ikEpmSJ/?utm_source=ig_web_copy_link) (28.09.2022).

by President Zelenskyy, of note is that, similarly to Putin, he often employs historical comparisons and references, which are well-suited to the place and circumstances and, most of all, to the audience. For example, in a speech given before the US Congress on March 16, 2022, he made references to many events of importance to Americans (such as the famous “I have a dream” speech by Martin Luther King). He also mentioned the momentous Japanese attack on Pearl Harbor and even the events of September 11, 2001.<sup>33</sup> When speaking in the Bundestag, he told members of the German Parliament that “a new wall built across Europe” had to be torn down.<sup>34</sup> When addressing the Kneset, he compared the war in Ukraine to the “final solution of the Jewish question”,<sup>35</sup> as the rulers of Nazi Germany referred to their plan of exterminating European Jews. Finally, when speaking to French members of the parliament, Volodymyr Zelenskyy recalled the tragedy of World War I and compared the siege of Mariupol to the “ruins of Verdun”.<sup>36</sup>

Although we can't unequivocally state that Vladimir Putin has ultimately lost the information war and the Russian communication and image strategy has been a failure, there can be no doubt that the Ukrainian President is doing an excellent job of using modern tools to pursue his chosen communication strategy.

## Summary

In summary, we can state that the analysis has led to the conclusion that the research hypotheses formulated earlier in the paper have mostly been confirmed. The first hypothesis (H1) that the Russian-Ukraine war is an example of a new approach to information war appears to be sound, as even if the methods and tools used to wage this war have been used before, social media has never been used on a similar scale. Although hostilities are still ongoing, many experts suggest that Ukrainians are win-

---

<sup>33</sup> “Przemówienie prezydenta Zełenskiego przed Kongresem USA”, *TVN24*, 16.03.2022, [on-line:] <https://tvn24.pl/swiat/prezydent-ukrainy-wolodymyr-zelewski-w-kongresie-usa-przemowienie-5637846> (28.09.2022).

<sup>34</sup> “Zełewski w Bundestagu: ‘Pomóżcie nam!’”, *Deutsche Welle*, 17.03.2022, [on-line:] <https://www.dw.com/pl/zelewski-w-bundestagu-pomozcie-nam/a-61158982> (28.09.2022).

<sup>35</sup> “Mocne przemówienie Zełenskiego w Knesecie: Izrael musi wybrać, kogo popiera”, *RMF24*, 20.03.2022, [on-line:] [https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-mocne-przemowienie-zelewskiego-w-knesecie-izrael-musi-wybrac,nId,5905657#crp\\_state=1](https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-mocne-przemowienie-zelewskiego-w-knesecie-izrael-musi-wybrac,nId,5905657#crp_state=1) (28.09.2022).

<sup>36</sup> “Wołodymyr Zełewski przed francuskim parlamentem: Europa od 80 lat nie widziała tego, co teraz dzieje się w Ukrainie”, *TVN24*, 23.03.2022, [on-line:] <https://tvn24.pl/swiat/ukraina-wolodymyr-zelewski-przed-parlamentem-francji-europa-od80-lat-niewidziala-tego-co-teraz-dzieje-sie-na-ukrainie-5646669> (28.09.2022).

ning the ongoing information war. It would appear that the second hypothesis (H2), positing that both sides of the conflict are using different methods of communication, is also true. Ukraine has been waging psychological warfare thanks to the activity of President Zelenskyy, who has been directly addressing political decision-makers and international public opinion, whereas communication by the President of the Russian Federation is much more limited and involves giving speeches which are not broadcast live. Activity on social media is implemented using the “troll army”. Although both sides of the conflict obviously use the same true and tested forms and means of communication (such as propaganda, post-truth and fake news), Ukraine has used propaganda more frequently to uncover disinformation rather than spread it. Another noticeable difference is the role in which both countries place themselves. The Russian Federation presents itself as a liberator of Ukrainians oppressed by their own government, while Ukraine keeps stressing and emphasising that it is the victim of criminal aggression. The last hypothesis (H3), stating that the information war waged during the Russia-Ukraine conflict is used to achieve military, political and economic goals, is also indisputable. Although both sides of the conflict use different methods of communication, they seek to achieve the same goals – primarily the strengthening of their desired image, which will enable the acceptance of their actions by the international community and assistance from key political decision-makers and help them strengthen both in terms of military power, and political and economic position in the world.

## References

- “Bielsat TV z serwisem informacyjnym po ukraińsku, portal Wot Tak zablokowany w Rosji”, *Wirtualnemedia.pl*, 9.03.2022, [on-line:] <https://www.wirtualnemedia.pl/arttykul/bielsat-informacje-wojna-w-ukrainie-rosja>.
- Coutau-Bégarie H., *Traité de strategie*, Economica, Paris 1999.
- “Cyberataki hakerów z Rosji na ukraińskie sieci komputerowe. Przejęli wrażliwe dane”, *Polsat News*, 16.02.2022, [on-line:] <https://www.polsatnews.pl/wiadomosc/2022-02-16/cyberataki-hakerow-z-rosji-na-ukrainskie-sieci-komputerowe-przejeli-wrazliwe-dane/>.
- Czeszejko S., Janczak J., “Militarne aspekty środowiska elektronicznego – próba rewizji istniejącej terminologii”, *Zeszyty Naukowe AON*, vol. 1, no. 98 (2015), pp. 78–81.
- “Doktryna Wojenna Federacji Rosyjskiej”, *bbn.gov.pl*, [on-line:] <https://www.bbn.gov.pl/ftp/dok/01/DoktrynaFederacjiRosyjskiej.pdf>.
- “Dzień Zwycięstwa 9 Maj 2022 r. Przemówienie Putina”, *YouTube*, [on-line:] <https://youtu.be/81IyVpv75o4>.
- Ellul J., *Propaganda: The Formation of Men's Attitudes*, Alfred A. Knopf, New York 1973.

- “Elon Musk”, *Twitter*, [on-line:] [https://twitter.com/elonmusk/status/1497701484003213317?ref\\_src=twsrc^tfw|twcamp^tweetembed|twterm^1497701484003213317|twgr^96d348165aad556abbe2ad6b109dbb59de6aaa68|twcon^s1\\_c10&ref\\_url=](https://twitter.com/elonmusk/status/1497701484003213317?ref_src=twsrc^tfw|twcamp^tweetembed|twterm^1497701484003213317|twgr^96d348165aad556abbe2ad6b109dbb59de6aaa68|twcon^s1_c10&ref_url=).
- Foxall A., “In Putin’s Russia, History Is Subversive”, *The American Interest*, 6.06.2016, [on-line:] <https://www.the-american-interest.com/2016/06/06/in-putins-russia-history-is-subversive>.
- “Google znów ukarany w Rosji. 387 mln dol. kary za nieusuwanie treści”, *Business insider*, 18.07.2022, [on-line:] <https://businessinsider.com.pl/technologie/nowe-technologie/google-ukarany-w-rosji-387-mln-dol-kary-za-nieusuwanie-tresci/4s6wkz3>.
- Grodzki R., *Wojna gruzińsko-rosyjska 2008: przyczyny, przebieg, skutki*, Wydawnictwo Replika, Zakrzewo 2009.
- Irisova O., “A Lie is the Truth, Intersection Project”, *Intersection Project*, 3.07.2015, [on-line:] <http://intersectionproject.eu/article/society/lie-truth>.
- “Katarzyna Włodkowska”, *Twitter*, [on-line:] [https://twitter.com/k\\_wlodkowska/status/1497452572784824320?s=20&t=bI6TdOKqvCd3uDOxPEMwLg](https://twitter.com/k_wlodkowska/status/1497452572784824320?s=20&t=bI6TdOKqvCd3uDOxPEMwLg).
- Irisova O., “A Lie is the Truth, Intersection Project”, *Intersectionproject*, 3.07.2015, [on-line:] <http://intersectionproject.eu/article/society/lie-truth>.
- Kaźmierczak D., “Walka informacyjna we współczesnych konfliktach i jej społeczne konsekwencje”, *Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate et Educatione Civili*, vol. 7 (2017), pp. 111–129, <https://doi.org/10.24917/20820917.7.7>.
- Kruglashov A., Shvydiuk S., “Hybrydowe zagrożenia dla demokracji. Wybrane przykłady zewnętrznej ingerencji Rosji w wybory”, *Wschód Europy. Studia Humanistyczno-społeczne*, vol. 6, no. 2 (2020), pp. 79–92, <https://doi.org/10.17951/we.2020.6.2.79-93>.
- Maciejak M., *Anatomia konfliktu rosyjsko-czeczeńskiego. Grozny 1994/1995, 1999/2000*, Infortitions, Zabrze–Tarnowskie Góry–Połomia 2018.
- “Meta’s Adversarial Threat Report: First Quarter 2022”, *Meta*, 7.04.2022, [on-line:] <https://about.fb.com/news/2022/04/metad-adversarial-threat-report-q1-2022>.
- “Mocne przemówienie Zelenskigo w Knesecie: Izrael musi wybrać, kogo popiera”, *RMF24*, 20.03.2022, [on-line:] [https://www.rmfm24.pl/raporty/raport-wojna-z-rosja/news-mocne-przemowienie-zelenskigo-w-knesecie-izrael-musi-wybrac,nId,5905657#crp\\_state=1](https://www.rmfm24.pl/raporty/raport-wojna-z-rosja/news-mocne-przemowienie-zelenskigo-w-knesecie-izrael-musi-wybrac,nId,5905657#crp_state=1).
- “Orędzie Putina: pochwały, obietnice i pogróżki”, *Ośrodek Studiów Wschodnich im. Marka Karpią*, 21.04.2021 [on-line:] <https://www.osw.waw.pl/pl/publikacje/analizy/2021-04-21/orędzie-putina-pochwały-obietnice-i-pogrozki>.
- Parfitt T., “My Life as a pro-Putin Propagandist in Russia’s Secret Troll Factory”, *The Telegraph*, 24.06.2015, [on-line:] <https://www.telegraph.co.uk/news/worldnews/europe/russia/11656043/MyLife%20as-a-pro-Putin-propagandist-in-Russias-secret-troll-factory/>.
- “Przemówienie prezydenta Zelenskigo przed Kongresem USA”, *TVN24*, 16.03.2022, [on-line:] <https://tvn24.pl/swiat/prezydent-ukrainy-wolodymyr-zelenski-w-kongresie-usa-przemowienie-5637846>.
- Puto K., “Na Ukrainie zamknęli internet”, *Krytyka Polityczna*, 19.05.2017, [on-line:] <https://krytykapolityczna.pl/felietony/kaja-puto/na-ukrainie-zamkneli-internet/>.
- Rozporządzenie Rady (UE) 2022/350 z dnia 1 marca 2022 r. w sprawie zmiany rozporządzenia Rady (UE) nr 833/2014 dotyczącego środków ograniczających w związku z działaniami Rosji destabilizującymi sytuację na Ukrainie*, [on-line:] <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:32022R0350&from=EN>.

- “Russia Today i Sputnik blokowane w Europie. Tak Unia walczy z rosyjską propagandą”, *Business Insider*, 9.03.2022, [on-line:] <https://businessinsider.com.pl/biznes/russia-today-i-sputnik-blokowane-w-europie/p56dt93>.
- Schwartau W., *Information Warfare: Protecting Your Personal Security in the Computer Age*, Thunder’s Mouth Press, New York–Emeryville, CA 1996.
- Smith B., *Defending Ukraine: Early Lessons from the Cyber War*, 22.06.2022, [on-line:] <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/>.
- Sokała W., “Przyjaciele Putina: Watykan i kto jeszcze”, *Microsoft*, 22.01.2022, [on-line:] <https://www.gazetaprawna.pl/wiadomosci/swiat/artykuly/8413152,jakie-panstwa-popieraja-rosje-i-dlaczego-onz.html>.
- “WKontaktie, największy serwis społecznościowy Rosji, trafił w ręce osób związanych z Putinem”, *Komputer Świat*, 6.12.2021, [on-line:] <https://www.komputerswiat.pl/aktualnosci/wydarzenia/wkontaktie-najwiekszy-serwis-spolesznosciowy-rosji-trafil-w-rece-osob-zwiazanych-z/7cnjx60>.
- “Wojna na Ukrainie? Orędzie Putina z 21.02.2022”, *YouTube*, [on-line:] <https://youtu.be/uN85c2jeAtM>.
- “Wołodimir Zelenski przed francuskim parlamentem: Europa od 80 lat nie widziała tego, co teraz dzieje się w Ukrainie”, *TVN24*, 23.03.2022, [on-line:] <https://tvn24.pl/swiat/ukraina-wolodymyr-zelenski-przed-parlamentem-francji-europa-od80-lat-niewidziala-tego-co-teraz-dzieje-sie-na-ukrainie-5646669>.
- “ZelenskyyUa”, *Twitter*, [on-line:] [https://twitter.com/ZelenskyyUa/status/1497450853380280320?s=20&t=FEJfWBJdXRL\\_gZLKi0toQg](https://twitter.com/ZelenskyyUa/status/1497450853380280320?s=20&t=FEJfWBJdXRL_gZLKi0toQg).
- “Zelenskiy Official”, *Instagram*, [on-line:] [https://www.instagram.com/reel/Ch24ikEpmSJ/?utm\\_source=ig\\_web\\_copy\\_link](https://www.instagram.com/reel/Ch24ikEpmSJ/?utm_source=ig_web_copy_link).
- “Zelenski w Bundestagu: „Pomóżcie nam!””, *Deutsche Welle*, 17.03.2022, [on-line:] <https://www.dw.com/pl/zelenski-w-bundestagu-pomozcie-nam/a-61158982>.



## The Russian Narrative Construct towards Ukraine

**ABSTRACT:** The article focuses on revealing various civilisational-cultural ('Russian order', triune Ruthenian nation, Moscow – third Rome), geopolitical (Ukraine as an axis of European stability, a fragment of the so-called “convergence zone”, with features of a zone disorganised by conflict and internal fragmentation – crush zone, the concept of Russia – island) and intrasystemic (totalitarian tendencies) elements of the Russian narrative message towards Ukraine of the time of the second, great aggression (2022). The article refers to the notion of totalitarian political gnosis as a product of totalitarian reality that justifies social mobilisation against an acknowledged hostile target – in this case, an independent, struggling Ukraine with the possibility of sovereign choice of development path. The analysis refers to the historical approach and the paradigm of critical geopolitics, deconstructing the narrative that contributes to geopolitical perceptions and the geopolitical image of reality. To substantiate the claim of a totalitarian political gnosis conditioning the official narrative, reference was made to Vladimir Putin's speech on February 21, 2022, constituting the decision to aggress against Ukraine.

**KEYWORDS:** Ukraine, The Russian Federation, geopolitics, the “Russian order”, totalitarian political gnosis

## Introduction

On February 24, 2022, the second invasion of Ukraine by the Russian Federation (RF), with its onset truly devastating for regional and global stability, modified the hierarchy of global concerns and, once again – in a symbolic sense – made Moscow the capital of the aggressor state and the essential reference point for attempts to understand the determinants of the tragic events. Natural in this context, the need to rationalise the actual state of the war had to include a search for the causes of an act which, in the face of the problems of global climate catastrophe, increased migration. The fight against terrorism appeared to be a distant reality, arousing a real, long absent and overwhelming fear for the future. The so-called “special military operation” in Ukraine announced by Russian President Vladimir Putin on the day of the invasion was the breath of a broader narrative, the relatively clear message of which, involving the demand to protect the Russian-speaking population from the humiliation and extermination that was supposed to be the work of alleged Banderites and neo-Nazis (for example),<sup>1</sup> results in a search for justification for the efforts to explain the motives behind the Russian Federation’s initiation of the military action. This allows a conclusion in the form of an important premise for the study, stating that the fact of a large-scale, second Russian invasion of Ukraine was probably associated not only with the geopolitical interests of the aggressor here (e.g., the likely desire to gain territorial access to the quasi-state of Transnistria)<sup>2</sup>, but also stemmed from a sense of violation of certain values or visions of international relations and/or the model of national or social existence.

This analysis aims to reflect on the axiological and subject-oriented architecture of Russian news coverage of fundamental importance to the war against Ukraine. For this reason, elements of the information stream rooted in the Russian tradition of political, geopolitical and foreign policy thought will be examined, forming an integral narrative of the Russian order (“*russkij mir*”) – a historically, culturally, ethically and politically grounded vision, the objectivity of which is understood in terms of the threat of Western civilisational action. Specifically, the following hypothesis is adopted

---

<sup>1</sup> R. Treisman, “Putin’s Claim of Fighting against Ukraine ‘Neo-Nazis’ Distorts History, Scholars Say”, *NPR*, 1.03.2022, [on-line:] <https://www.npr.org/2022/03/01/1083677765/putin-denazify-ukraine-russia-history> (23.09.2022).

<sup>2</sup> See more: M. Kosienkowski, *Naddniestrzańska Republika Mołdawska. Determinanty przetrwania*, Wyd. Adam Marszałek, Toruń 2010; P. Oleksy, *Naddniestrze. Terror tożsamości*, Wyd. Czarne, Wołowiec 2018.

for the study: *The main threads of the Russian narrative in the context of the current aggression against Ukraine are based on a totalitarian mindset (totalitarian political gnosis).*

The consequence of the assumption formulated above is the identification of an auxiliary issue, according to which the Russian civilisation-state project in the context of the Gnostic perception of reality is unique, consisting of recognising this project as clearly positive and, thus, classifying this phenomenon on the side of good. A parallel conclusion that meets the condition for the existence of ontological dualism resulting from political gnosis is the statement that Ukraine and Ukrainians are representatives of a negative, evil – but necessary – world for the binary structure of reality.

The first part of the analysis will present a set of various civilisational, historical, geopolitical and systemic conditions that contributed to the perception of the “Russian order” as threatened by the Western forces of the ideal world. The second part presents selected strands of the Russian narrative, which – fulfilling the condition of totalitarian, Gnostic newspeak – situate Ukraine on the side of hostile forces that threaten Russia as the depository of the proper truth.

The study was based on the model of critical geopolitics, the main idea of which is the deconstruction of geopolitical perceptions and the resulting geopolitical world picture. The historical approach in political science and the categories of analysis of non-democratic systems, especially the empirical phenomenon of political gnosis, will be applied for this purpose. The elements of formal geopolitics, based on primary (speeches and opinions) and secondary (scientific studies) sources, and the threads of practical geopolitics – based on political opinions and actions – will be critically analysed.

## Architecture of aggression – geopolitics, geocivilisation, axiology and practice

In one of his final analyses, which was an attempt at a model interpretation of changes in the so-called “Eurasian Convergence Zone”, the eminent American geographer and geopolitician Saul B. Cohen noted that, for historical reasons connected with the formation of Kievan Rus, at the turn of the ninth and tenth centuries as an area encompassing today’s European part of Russia – as well as Belarus and Ukraine – the latter (i.e., Ukraine), often a zone of later conflicts, plays a very important role when it comes to ‘Russian national feelings’.<sup>3</sup> According to Cohen, Ukraine was and is con-

---

<sup>3</sup> Cf.: S.B. Cohen, “The Eurasian Convergence Zone: Gateway or Shatterbelt?”, *Eurasian Geography and Economics*, vol. 46, no. 1 (2005), pp. 6–7.

sidered an integral part of the embryonic area of the modern Russian state. This gives rise, after all, to a categorical statement based on historical reasoning and, therefore, inherently containing civilisational themes. Cohen points out that the so-called “Kievan Rus” was a country held together by an element of Slavic ethnicity and an orthodox Christian religion – Eastern Orthodox Christianity (Slavic and Orthodox Christian state).<sup>4</sup> This view of Cohen is accompanied by another, geostrategic nature, ascribing to Russia the traditional perception of Ukraine as an area naturally susceptible to clash with Western forces due to its location at the country’s southern edge. This has the consequence of attributing the character of a borderland to Ukrainian land, a natural consequence of which is constant pressure from other centres of power giving the area of Ukraine the characteristics of a so-called “crush zone”.<sup>5</sup> A crush zone is an area that is internally disorganised and subject to objective conflict between rival actors representing the major powers – in this case, the Western states institutionalised by the EU, NATO and the Russian Federation.

The geopolitical positioning of Ukraine applied by Cohen coincides with the conclusions of a more predictive and practical geostrategic nature formulated by Zbigniew Brzezinski. In his seminal study of the formula of the post-Cold War international order, Brzezinski not only recognised Ukraine as a key element of the European equilibrium, but also as a decisive factor in the possibility of restoring Russia’s imperial influence – which, after the collapse of the USSR, created a geopolitical vacuum in the middle of the Eurasian continent.<sup>6</sup> This role stems from the qualification of the Ukrainian state as a geopolitical pivot whose fundamental position is based not on strength or ambition, in this case Kiev, but on a key geographic location and an internal situation that directly affects the actions of the world’s great powers.<sup>7</sup>

The above definition of Ukraine’s key role turned out to be the most important premise for Brzezinski’s later opinion, dating from 2012 (i.e., just before the first Russian invasion of Ukraine), in which he not only classifies the aforementioned state as part of the set of international actors most threatened geopolitically, but also draws what turned out to be the correct scenario of events (i.e., the eventuality of Russian armed aggression and resistance, amplified by a growing Ukrainian national consciousness, distinct from the Russian one)<sup>8</sup>.

---

<sup>4</sup> *Ibidem*, p. 7.

<sup>5</sup> *Ibidem*; *idem*, *Geopolitics: The Geography of International Relations*, Rowman & Littlefield, Maryland 2015, p. 48.

<sup>6</sup> Z. Brzeziński, *Wielka szachownica*, Bertelsmann Media, Warszawa 1999, pp. 86, 88–119.

<sup>7</sup> *Ibidem*, p. 41.

<sup>8</sup> Cf.: *idem*, *Strategiczna wizja. Ameryka a kryzys globalnej potęgi*, Wydawnictwo Literackie, Kraków 2013, pp. 130–132.

Both Cohen's and Brzezinski's approaches clearly bear the hallmarks of a realist approach in the study of international relations, recognising the causal role of the main players (i.e., the states) which, in a system characterised by conditions of anarchy, are essentially aiming for survival. In this context, economic theories of organisational development are all too noticeable.<sup>9</sup>

In the above view, Ukraine becomes a function of the essence of the current force relationship of the major world powers – mainly the US, the EU and the Russian Federation aiming at: the continuous, subjective strengthening of the Euro-Atlantic system through the formal and procedural incorporation of new members into existing civilian and military structures, and the restoration of the former Soviet Union's sphere of influence and their expansion through the adoption of a formula of a universal, Russian-centric order (*rususkij mir*).

The attempt to justify and promote another world centre of power with autotelic features after the USA, China and the EU does not only result from the Russian tradition of geopolitical thought – which, in the eyes of its contemporary representatives (e.g., Igor Panarin<sup>10</sup> or Alexander Dugin)<sup>11</sup> – but it also becomes a contribution to the resistance against the expansion of the influence of the USA and its allies deeper into Eurasia and an element of building a new, multipolar international order with a significant role of Eurasian entities (i.e., Russia and China). The main thing is the recognition of the civilisational principals that fundamentally differentiate Russia from the countries of the West, which are considered a fundamental threat because of values such as pernicious liberal individualism.<sup>12</sup> Therefore, the construction and use of certain myths of a geocivilisation nature<sup>13</sup> are based on the assumption of the proper legitimisation of state power based on true tradition – which is, therefore, entitled to create a universal system. Such conditions are met by the doctrine of Moscow – the

---

<sup>9</sup> Cf.: K.N. Waltz, *Theory of International Politics*, Addison-Wesley Publishing Co., Reading, Massachusetts 1979, pp. 88–92.

<sup>10</sup> Cf.: J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej. Między nauką, ideologicznym dyskursem a praktyką*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2010, pp. 286–289.

<sup>11</sup> Cf.: P. Eberhardt, "Koncepcje geopolityczne Aleksandra Dugina", in P. Eberhardt, *Słowińska geopolityka. Twórcy rosyjskiej, ukraińskiej i czeskosłowackiej geopolityki oraz ich koncepcje ideologiczno-terytorialne*, Wyd. Arcana, Kraków 2017, pp. 342–347.

<sup>12</sup> J. Diec, "Doktryna rosyjskiej polityki zagranicznej. Partnerzy najbliżsi i najdalsi", in *Geostrategiczny wybór Rosji u zarania trzeciego tysiąclecia*, vol. 1, Wyd. Uniwersytetu Jagiellońskiego, Kraków 2015, p. 149.

<sup>13</sup> When I use the term 'geo-civilisational myth', I am referring to a concept that evaluates a particular geographical space, in this case Russia, because of the ascribed existence of certain cultural characteristics deemed appropriate and desirable.

third Rome, referring to the claims of the monk of the Orthodox Church Philotheus that, due to heresy attributing to Christ the acquisition of human nature, the proper (first) Rome fell and then, as a result of the alliance with him, also the second (i.e., Constantinople). The third Rome is Moscow, portrayed as the centre and mainstay of the universalist Christian tradition.<sup>14</sup> Joachim Diec provides excellent characteristics of the contemporary context in which the doctrine in question operates: “What is striking about the idea of Moscow – the third Rome, one of the most fundamental to the subsequent centuries of the existence of the Moscow state on the international stage, is its similarity to the perception of the capital as a kind of centre of the world, *axis mundi*, through the conviction of its own one-ness, uniqueness. At the same time, however, this belief is devoid of inner certainty, no lasting peace (...). The outside world is seen as a threat, but also as an environment that needs to be convinced of its own superiority. Hence, the strictly monocentric doctrine constantly struggles with the awareness of the lack of recognition from the international environment.”<sup>15</sup>

The claim of Russia as the sole, traditionally legitimised and representative of the true principles of Christian civilisation and, therefore, universal centre of state power justifies the tendency to octroi [dictate] desirable solutions – especially to those entities considered native or in the orbit of direct influence. Therefore, the adoption of the concept of the triune Ruthenian nation, composed of ethnic Russians (Great Russians) and Belarusians and Ukrainians (Lesser Russians), was a natural consequence of not only the sacred principle of transferring power from Rome to Moscow, but also the recognition of the supreme role of Orthodoxy and the Russian state in building a political community.<sup>16</sup> In this obvious, eclectic vision of the nation, the Russians were given priority, while the remaining groups – as partially Latinised and thus detached from the true Orthodox homeland – were placed lower, also by recognising their peasant origin, suggesting a lower social level.<sup>17</sup>

The formula of national unity, with an evident element of supremacy and subordination of other communities and considered to be the chief of the Orthodox Russian nationality, omitted the element of both national aspirations and the state-building process in relation to Belarusians and Ukrainians in particular. This does not change the fact that the principle of unity survived and was strengthened even despite several decades of the communist system, which saw the creation of a communist-Soviet

<sup>14</sup> Cf.: J. Diec, *op. cit.*, p. 37.

<sup>15</sup> *Ibidem*, pp. 37–38.

<sup>16</sup> Cf.: R. Radzik, “Rosyjska wizja narodu ogólnoruskiego”, *Studia Białorutenistyczne*, vol. 10 (2016), pp. 56, 60–61.

<sup>17</sup> *Ibidem*, p. 61.

nation based on the existing ethnos – the main initiator and executor of which, as in the periods preceding communism, was the centralised state apparatus. Paradoxically, as Ryszard Redzik points out, the demarcation of the borders of the Soviet republics, the development of national languages (in spite of parallel Soviet Russification, or the separate state-like status of Belarus and Ukraine at the UN) contributed to the strengthening of the emancipation aspirations of these societies, regarded by Russians as members of the same all-Russian and Orthodox community, but not as equal representatives of a *de facto* provincial, inferior culture.<sup>18</sup>

The imposed sense of national unity interacted with the undemocratic features of the Russian/Soviet state. The system of imperial, tsarist one-man rule and then Soviet totalitarianism – which reached its climax under Joseph Stalin<sup>19</sup> – found its continuation in the retreat from the reformist, West-cooperative model of hard authoritarianism presented by Vladimir Putin. Initially, the conditions for this were created by the Constitution of the Russian Federation adopted in 1993, introducing a super-presidential system of power in which the head of state, who represented an extremely strong executive power at the expense of legislation, gained supremacy over all other state structures. Moreover, although the source of power was assigned to the multi-ethnic nation of the Russian Federation, only the President of the Federation represented this power, guaranteeing its unity and being based on the constitutional act. The practice of Putin's long-standing rule as head of state, which lasted with a four-year break in the 2008-2012 period from 1999 until the present time, turned out to have a decidedly anti-democratic and neo-despotic face. This can be evidenced not only by the fight against the opposition – here, in addition to individual repressions against its representatives (e.g., Mikhail Khodorkovsky, Alexei Navalny), collective repressions that turned many NGOs into alleged agent centres linked to Western forces,<sup>20</sup> or the falsifications and numerous cases of abuse in the elections of the Russian State Duma (e.g., in 2011 and 2021)<sup>21</sup> – but also the fundamental legal and institutional changes

---

<sup>18</sup> *Ibidem*, pp. 61–62.

<sup>19</sup> According to Russian political scientist Yuli Zolotovskiy, the system of totalitarian Stalinism was based on two features: omnipresence and a repressive-punitive orientation as indispensable determinants of the actions of the essential element of the undemocratic order - the totalitarian bureaucracy. The latter was the basis of a state of total tyranny imposing universal terror – com: *Rosja. XX wiek. Od utopii komunistycznej do rzeczywistości globalistycznej*, transl. P. Burek, Wyd. Uniwersytetu Jagiellońskiego, Kraków 2004, pp. 78–85.

<sup>20</sup> M. Łojkowska, “Agenci społeczeństwa. Ustawy o zagranicznym finansowaniu w Rosji”, *NGO.pl*, 23.10.2020, [on-line:] <https://publicystyka.ngo.pl/agenci-spoleczenstwa-ustawy-o-zagranicznym-finansowaniu-w-rosji> (7.10.2022).

<sup>21</sup> J. Rogoża, “Rosja po wyborach: oddolna presja zmusza władze do zmiany taktyki”, *OSW*, 14.12.2011, [on-line:] <https://www.osw.waw.pl/pl/publikacje/analizy/2011-12-14/rosja-po-wyborach->

undertaken at the turn of 2019/2020. The constitutional reform that was then carried out was a fundamental step towards the legally unlimited (in term) extension of Putin's holding of office as Head of State and towards an even stronger supremacy of the President over the government and the judicial system.<sup>22</sup>

Inherited and developed along with social, legal and institutional traditions and the usually undemocratic practice of exercising power, the Russian model of governing and arranging international relations is saturated with constant tendencies towards the autocratic promotion of civilisational values considered specific – Orthodoxy, Russian national-territorial unity and a particularly cohesive policy of building the so-called “Russian order”, alternative to Western liberal openness (*ruskij mir*, Russian world).

The term itself had already existed in Russian politics since the early 1990s, when Boris Yeltsin and Andrei Primakov introduced into the discourse the formal-legal category of ‘compatriots abroad’, which at the time meant individual persons who, as a result of the break-up of the USSR, remained outside the borders of the Russian Federation, felt a historical, cultural and linguistic connection to Russia regardless of their current citizenship.<sup>23</sup> The situation has changed with the geostrategic evolution of the situation in Russia's so-called “near abroad”, which can be definitely linked to the process of expanding US and NATO influence in the former Soviet republics (e.g., the Baltic states) that were admitted to the Alliance in 2004. Of particular importance were the years 2007–2008, when the actions of pro-Western-minded Georgia and Ukraine were aimed at gaining membership of the North Atlantic Treaty Organisation (NATO), while Russia implemented what was most likely a previously prepared plan to regain influence in the former Soviet area. The result was a Russian-Georgian war lasting several days, taking advantage of the existence of pro-Russian separatists in Abkhazia and South Ossetia.

The events of 2008 and the Russian decision on aggression in Ukraine – resulting in the incorporation of Crimea, including the actual detachment, destabilisation and subsequent recognition of the so-called “People's Republic of Donetsk and Luhansk” – transformed the idea of cultural and historical connection into an element of

---

oddolna-presja-zmusza-wladze-do-zmiany-taktyki (7.10.2022); H.A. Conley, A. Lohsen, “Where Does Russian Discontent Go from Here? Russia's 2021 Election Considered”, *CSIS*, 23.09.2021, [on-line:] <https://www.csis.org/analysis/where-does-russian-discontent-go-here-russias-2021-election-considered> (7.10.2022).

<sup>22</sup> Cf.: M. Domańska, “Wieczny Putin' i reforma rosyjskiej konstytucji”, *OSW*, 13.03.2020, [on-line:] <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-03-13/wieczny-putin-i-reforma-rosyjskiej-konstytucji> (7.10.2022).

<sup>23</sup> I.A. Zevelev, “The Russian World Boundaries”, *Russia in Global Affairs*, 7.06.2014, [on-line:] <https://eng.globalaffairs.ru/articles/the-russian-world-boundaries/> (8.10.2022).

the politics of a force trying to revive powers. These powers are defined henceforth as action based on various means, civil and military, aimed at reintegrating the territories of the former Soviet Union and connecting with areas inhabited by people who feel communal with Russian culture and civilisation.<sup>24</sup>

The evolution of Russian policy after the unsuccessful experiment with pro-Western reforms in the 1990s, therefore, returned to the tracks of isolationism and autarky under Putin,<sup>25</sup> which had to be combined with the strengthening of internal security policy – understood as the regaining and centralisation of influence in the area of the so-called “near abroad”.<sup>26</sup> The application of the principle of “Russian order”, which, apart from military measures, also assumed wider activities (e.g., related to the promotion of language and culture)<sup>27</sup> can be safely considered the dominant doctrine in Russian foreign policy, combining both hard and soft forms of state power and the native principle of organising areas recognised as gravitating towards Russian culture.

---

<sup>24</sup> *Ibidem.*

<sup>25</sup> A certain convergence with the principle of the ‘Russian order’ understood in terms of the so-called ‘near abroad’ can be seen in Vadim Tsymbursky’s concept of Russia – the island, which assumed, like the concept of Moscow – the Third Rome, the existence of an independent and autonomous civilisation, immune to threats through the appropriate organisation of buffer zones, the so-called ‘land straits’, separating Russia from the main civilisational centres of Europe and Asia. Tsymbursky attributed special importance to the so-called Great Limitrophe stretching from Finland in the north, through Eastern Europe and Central Asia to Korea, which was supposed to safeguard Orthodox civilisation from internal turbulence and external attack – Cf.: J. O’Loughlin, P.F. Talbot, “Where in the World is Russia? Geopolitical Perceptions and Preferences of Ordinary Russians”, *Eurasian Geography and Economics*, vol. 46, no. 1 (2005), p. 24.

<sup>26</sup> An interesting interpretation of the ‘Russian world’ is formulated by Marek Budzisz, who argues that territorially, the known principle can be interpreted as an archipelago of links, incorporating e.g. Armenia or Syria into Russian civilisation and not necessarily Slavic or Russian-speaking national entities, as a ‘cultural and political gravitation towards Russia’ is sufficient – M. Budzisz, *Wszystko jest wojną. Rosyjska kultura strategiczna*, Wyd. ZonaZero, Warszawa 2021, p. 235.

<sup>27</sup> A significant instrument of institutional and cultural influence is the Russkiy Mir Foundation, deriving its origins from the words of V. Putin addressed to the Russian Federal Assembly in 2007, which defined the ‘Russian world’ as a ‘living space’ that goes beyond the borders of Russia itself, in principle encompassing those who use Russian as their own language, but also those who expressed a desire to learn about Russian culture (in this context, one can see a similarity with the official mission and activities of the British Council, the French Institute, the Goethe Institute or the Confucius Institute). The composition of the Foundation’s Board of Trustees is also not without significance, including the head of the Russian Ministry of Foreign Affairs, Sergei Lavrov, deputy head of the administration of the Russian president, Dmitry Kozak, and the minister of education of the Russian Federation, Sergei Kravtsov – Cf.: “About Russkij Mir Foundation”, *Russkiymir*, [online:] <https://russkiymir.ru/en/fund/index.php> (10.10.2022).

## ‘Russkij mir’ in action: Elements of the narrative legitimising the Russian Federation’s second aggression against Ukraine

In 2007, during a session of the Federal Assembly of the Russian Federation, President Vladimir Putin initiated state actions of the Foundation of the Russian Order (*Russkij Mir Foundation*). In addition to emphasising the concept of ‘Russian order’ as a zone of presence and active use of the Russian language (already mentioned in this work), he said that language is a “common heritage of many people”<sup>28</sup> and, as such, would never become a code for “hatred, hostility, xenophobia or isolationism”.<sup>29</sup> It would be peculiar to combine the considerations on the spatial role of the cultural code with pejorative phenomena characteristic of societies or the international system, but when applying the assumption of the existence of a totalitarian narrative based on political gnosis, this relationship acquires its proper meaning.

The use of a Gnostic-type political narrative stems from the process of creation of a new human being, *homo sovieticus*,<sup>30</sup> developed over time, revolutionary in its nature, accompanying the construction and functioning of a totalitarian system – in this case, the USSR. It is not the time to decide here about the fact and scope of a possible transfer of the model and attitude to contemporary Russia. Nevertheless, the presence of significant features of the political system, already indicated in this work – and especially the category of political thinking and communication – is a sufficiently serious contribution to assume that the continuation of at least part of the totalitarian reality is objective in nature.

Totalitarian political gnosis, referring to the traditional categories of Manichaeism, organises ideas based on ontological dualism – the contradiction between the world of good and evil. In this perspective, the whole reality is classified into its positive and negative manifestations, which unambiguously not so much makes it understandable and explainable, but reduces thinking to basic categories, truth and falsehood.<sup>31</sup>

Gnosis of the totalitarian type is characterised by distinctive categories that, in effect, create a specific structure. These include the over-interpretation of history, the

<sup>28</sup> “RMFound: Creation”, *Russkiimir*, [on-line:] <https://russkiimir.ru/en/fund/> (10.10.2022).

<sup>29</sup> *Ibidem*.

<sup>30</sup> About *homo sovieticus* see: H. Arendt, *Korzenie totalitaryzmu*, Wyd. Akademickie i Profesjonalne, Warszawa 2008; J. Staniszkis, *Ontologia socjalizmu*, Wyd. Dante, Wyższa Szkoła Biznesu, Kraków–Nowy Sącz 2006; A. Walicki, *Marksizm i skok do królestwa wolności*, Wyd. PWN, Warszawa 1996.

<sup>31</sup> Por.: R. Bäcker, *Nietradycyjna teoria polityki*, Wyd. Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2011, p. 191.

subordination of morality to the goal of action, the one-sided evaluation of man only in terms of the ability to participate in the world of good (either temporal or eternal salvation), the definition of the believer-fighter who, for the sake of participation in the attainment of right knowledge, renounces needs and acts only professionally.<sup>32</sup> In particular, from the totalitarian gnosis as a feature of social consciousness stems the conviction that there is an objective enemy and an imaginary entity, which manifests itself in specific newspeak.<sup>33</sup>

In our case, the imaginary being analysed in the first part was the triune Ruthenian nation's community that crossed the Russian Federation border drifting towards totalitarianism. However, for further consideration, it is assumed that the category of the objective enemy includes Ukraine and Ukrainians as part of a larger, hostile whole – the civilisation of the West. The assumption will be exemplified by reviewing the content of Russian President Vladimir Putin's speech on February 21, 2022, constitutive for the creation of the enemy,<sup>34</sup> preceding the second invasion of Ukraine.

In an evocative speech, saturated with many examples from history, economics, political systems, etc., Mr Putin clearly constructed a dichotomous division of reality using the Gnostic category of 'us' and 'them' while focusing more, understandably, on the characteristics of the enemy. As for the category created as one's own, positive, placed on the side of the good, we are dealing with reference to the connection with compatriots in Ukraine, but not treated as a formally and materially separate foreign country, but as a specific common historical, cultural and spiritual space, belonging from time immemorial and, therefore, always to the "Old Ruthenian" lands. Thus, the narrative shows some recognition of Ukraine's statehood – the speech included words about 'respecting the dignity and sovereignty of Ukraine', which, however, after 1991 – and at the request of its political elite – was to be given extensive and comprehensive economic assistance, with which Putin underlined the significant ties of cooperation. The inhabitants of Ukraine, and especially those from the south-eastern

---

<sup>32</sup> *Ibidem*, pp. 191–192.

<sup>33</sup> Idem, "Kategorie teoretyczne totalitaryzmu a badania empiryczne", *Studia nad Autorytaryzmem i Totalitaryzmem*, vol. 38, no. 2 (2016), pp. 14–15. It should be noted that the phenomenon of political gnosis itself has awaited methodological operationalisation. By distinguishing a comprehensive, empirical set of detailed categories that condition the objectivity of political gnosis – See: J. Rak, "How to Measure Political Gnosis? Empirical Evidence from Putin's Russia", *Przegląd Polityczny*, no. 4 (2017), pp. 159–171. The aforementioned collection was used in another analysis devoted to Vladimir Putin – see: A. Maćkowiak, "Elementy gnozy politycznej w orędziach Władimira Putina do Zgromadzenia Federalnego w latach 2014–2016", *Refleksje*, no. 19–20 (2019), pp. 153–168.

<sup>34</sup> "Address by the President of the Russian Federation", *Official Internet Resources of the 'President of Russia'*, 21.02.2022, [on-line:] <http://en.kremlin.ru/events/president/transcripts/67828> (11.10.2022).

part of the country, were considered to be friendly to the idea of cooperation with Russia. Therefore, those “millions” accepted “good relations with Russia” and “cultural and linguistic diversity”. Thus, it can be clearly stated that the historical model of one nation gathering together culturally and regionally similar ethnos is considered ideal and constitutes a reference point for the enemy personifying the forces of evil.

The design of the hostile side is more complex. It involves admitting historical mistakes (the artificial division of nations by inadequate borders of the USSR republics, which created *de facto* nation-states), mistaken political concepts (the Leninist model of strong autonomy of the republics with the possibility of breaking away from the federation) and political mistakes made at different times (the lack of centralist constitutional reform under communism or the misguided leadership of reforms in the 1980s). Thus, one can see the seemingly dual nature of the forces of evil – made up of self-inflicted errors but justified as not having been committed deliberately. In Putin’s judgment, they were the result of a very difficult situation (world war, revolution, economic collapse). The search for an answer to the question about the source of the negated state of affairs is the reference to the category of nationalism (fascism, neo-Nazism) – the source of which Putin sees in the Leninist principle of self-determination of nations. The alleged Ukrainian nationalism is accused of numerous offences such as repression and genocide against the Russian or Russian-friendly population, corruption, the oligarchisation of politics and the economy, leading to *coups d’état* and collaboration with obviously hostile, ‘Western capitals’ and their agendas – advisors and third sector organisations. Part of the expansion of the enemy category is to point to Ukraine’s institutional, material cooperation in military and security terms with the US and NATO, consisting of a range of activities. These include the adoption of what is considered to be an aggressive new Ukrainian military strategy, the installation of various forms (centres, bases) of NATO presence in Ukraine and the possible presence of ‘weapons of mass destruction’ on Ukrainian territory.<sup>35</sup>

In view of the above, the main enemy – Ukrainian nationalism, which is in the service of the self-interested, lying and aggressive USA and NATO, is a major threat to Russia. It shatters the unity of the historical, cultural and religious Ruthenian community, introduces an oppressive social system and threatens treaty-based and common-sense security principles. Worst of all, however, according to Putin, is the fact that Ukrainians are *de facto* going against their traditional, historical homeland,

<sup>35</sup> All quotes come from the English and Polish transcripts of Putin’s speech on February 21, 2022 – *ibidem*; “Współczesna Ukraina jest w całości dziełem Rosji”. Całe przemówienie Putina sprzed ataku”, *Gazeta Wyborcza*, 25.02.2022, [on-line:] <https://wyborcza.pl/magazyn/7,124059,28157005,wspolczesna-ukraina-jest-w-calosci-dzielem-rosji-cale-przemowienie.html> (11.10.2022).

Ruthenia. This is clearly expressed in the words: “Contemporary Ukraine is entirely the work of Russia, or more precisely, of Bolshevik, communist Russia. In fact, this process began shortly after the revolution of 1917, with Lenin and his comrades treating Russia very brutally, tearing away some of its historical territories. Of course, no one asked the millions of people who lived there (...). In fact, Ukraine did not have any solid traditions of true statehood. Since 1991, it has followed the path of mechanical copying of other people’s models, detached from both history and Ukrainian realities”<sup>36</sup>.

It is difficult to more clearly depreciate the feelings and community achievements of everyone who cultivates their individuality and the real tradition of striving for independence of a nation which, by failing to fit into the civilisation matrix of the world power, becomes the goal of its aggressive policy.

## Summary

The Russian concept of ‘*ruskij mir*’ is a specific state-cultural and historical construct, justifying the Russian Federation’s claim to what it considers to be the exclusive sphere of influence of the so-called “near abroad”, which includes the former Soviet republics, including Ukraine. The multi-level cooperation vision does not recognise a sovereign choice other than a development model similar to the Russian one. Therefore, any activity considered to be a deviation from the pattern of reintegration of the former Soviet space under Russian leadership is considered at least suspicious, if not overtly hostile in its nature. This fear is accompanied by the evolution of a strongly authoritarian political system under Vladimir Putin towards totalitarianism, excluding political and worldview pluralism. The consequence of this process is the emergence of a totalitarian political gnosis, manifested in language and attitudes, which assesses the values recognised by the Russian authorities and openly depreciates all those that deviate from the pattern. Therefore, adopting a dichotomous vision of reality has its geopolitical consequences (struggle for the sphere of influence and a renewed, relatively permanent division of the world), social (incapacitation and then attempts to mobilise a totally subordinated society) and cultural consequences, consisting of a return to the model of totalitarian culture and consciousness (*homo sovieticus*). Evolving towards totalism, the system seeks its justification; hence the objective character takes on a process of the permanent creation of the enemy manifested both in the sphere of communica-

---

<sup>36</sup> *Ibidem*.

tion and information as well as in aggressive actions. Ukraine, with its pro-European and pro-NATO aspirations, is currently such an enemy of the Russian Federation.

## References

- “About Russkij Mir Foundation”, *Ruskiymir*, [on-line:] <https://ruskiymir.ru/en/fund/index.php>.
- “Address by the President of the Russian Federation”, *Official Internet Resources of the ‘President of Russia’*, 21.02.2022, [on-line:] <http://en.kremlin.ru/events/president/transcripts/67828>.
- Arendt H., *Korzenie totalitaryzmu*, Wyd. Akademickie i Profesjonalne, Warszawa 2008.
- Bäcker R., “Kategorie teoretyczne totalitaryzmu a badania empiryczne”, *Studia nad Autorytaryzmem i Totalitaryzmem*, vol. 38, no. 2 (2016), <https://doi.org/10.19195/2300-7249.38.2.1>.
- Bäcker R., *Nietradycyjna teoria polityki*, Wyd. Naukowe Uniwersytetu Mikołaja Kopernika, Toruń 2011.
- Brzeziński Z., *Strategiczna wizja. Ameryka a kryzys globalnej potęgi*, Wydawnictwo Literackie, Kraków 2013.
- Brzeziński Z., *Wielka szachownica*, Bertelsmann Media, Warszawa 1999.
- Budzisz M., *Wszystko jest wojną. Rosyjska kultura strategiczna*, Wyd. ZonaZero, Warszawa 2021.
- Cohen S.B., “The Eurasian Convergence Zone: Gateway or Shatterbelt?”, *Eurasian Geography and Economics*, vol. 46, no. 1 (2005), pp. 6–7, <https://doi.org/10.2747/1538-7216.46.1.1>.
- Cohen S.B., *Geopolitics: The Geography of International Relations*, Rowman & Littlefield, Maryland 2015.
- Conley H.A., Lohsen A., “Where Does Russian Discontent Go from Here? Russia’s 2021 Election Considered”, CSIS, 23.09.2021, [on-line:] <https://www.csis.org/analysis/where-does-russian-discontent-go-here-russias-2021-election-considered>.
- Diec J., “Doktryna rosyjskiej polityki zagranicznej. Partnerzy najbliżsi i najdalsi”, in *Geostrategiczny wybór Rosji u zarania trzeciego tysiąclecia*, vol. 1, Wyd. Uniwersytetu Jagiellońskiego, Kraków 2015.
- Domańska M., “‘Wieczny Putin’ i reforma rosyjskiej konstytucji”, OSW, 13.03.2020, [on-line:] <https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2020-03-13/wieczny-putin-i-reforma-rosyjskiej-konstytucji>.
- Eberhardt P., “Konceptje geopolityczne Aleksandra Dugina”, in P. Eberhardt, *Słowińska geopolityka. Twórcy rosyjskiej, ukraińskiej i czechosłowackiej geopolityki oraz ich konceptje ideologiczno-terytorialne*, Wyd. Arcana, Kraków 2017.
- Kosienkowski M., *Naddniestrzańska Republika Mołdawska. Determinanty przetrwania*, Wyd. Adam Marszałek, Toruń 2010.
- Łojkowska M., “Agenci społeczeństwa. Ustawy o zagranicznym finansowaniu w Rosji”, *NGO.pl*, 23.10.2020, [on-line:] <https://publicystyka.ngo.pl/agenci-społeczenstwa-ustawy-o-zagranicznym-finansowaniu-w-rocji>.

- Maćkowiak A., "Elementy gnozy politycznej w orędziach Władimira Putina do Zgromadzenia Federalnego w latach 2014–2016", *Refleksje*, no. 19–20 (2019).
- O'Loughlin J., Talbot P.F., "Where in the World is Russia? Geopolitical Perceptions and Preferences of Ordinary Russians", *Eurasian Geography and Economics*, vol. 46, no. 1 (2005), pp. 23–50, <https://doi.org/10.2747/1538-7216.46.1.23>.
- Oleksy P., *Naddniestrze. Terror tożsamości*, Wyd. Czarne, Wołowiec 2018.
- Potulski J., *Współczesne kierunki rosyjskiej myśli geopolitycznej. Między nauką, ideologicznym dyskursem a praktyką*, Wyd. Uniwersytetu Gdańskiego, Gdańsk 2010.
- Radzik R., "Rosyjska wizja narodu ogólnorosyjskiego", *Studia Białorusinistyczne*, vol. 10 (2016), <http://dx.doi.org/10.17951/sb.2016.10.55>.
- Rak J., "How to Measure Political Gnosis? Empirical Evidence from Putin's Russia", *Przegląd Politologiczny*, no. 4 (2017), pp. 159–172, <https://doi.org/10.14746/pp.2017.22.4.13>.
- Rogoża J., "Rosja po wyborach: oddolna presja zmusza władze do zmiany taktyki", OSW, 4.12.2011, [on-line:] <https://www.osw.waw.pl/pl/publikacje/analizy/2011-12-14/rosja-po-wyborach-oddolna-presja-zmusza-wladze-do-zmiany-taktyki>.
- Staniszki J., *Ontologia socjalizmu*, Wyd. Dante, Wyższa Szkoła Biznesu, Kraków–Nowy Sącz 2006.
- Treisman R., "Putin's Claim of Fighting against Ukraine 'Neo-Nazis' Distorts History, Scholars Say", *NPR*, 1.03.2022, [on-line:] <https://www.npr.org/2022/03/01/1083677765/putin-denazify-ukraine-russia-history>.
- Walicki A., *Marksizm i skok do królestwa wolności*, Wyd. PWN, Warszawa 1996.
- Waltz K.N., *Theory of International Politics*, Addison-Wesley Publishing Co., Reading, Massachusetts 1979.
- "Współczesna Ukraina jest w całości dziełem Rosji. Całe przemówienie Putina sprzed ataku", *Gazeta Wyborcza*, 25.02.2022, [on-line:] <https://wyborcza.pl/magazyn/7,124059,2815700,5,wspolczesna-ukraina-jest-w-calosci-dzielem-rosji-cale-przemowienie.html>.
- Zevelev I.A., "The Russian World Boundaries", *Russia in Global Affairs*, 7.06.2014, [on-line:] <https://eng.globalaffairs.ru/articles/the-russian-world-boundaries/>.
- Zołotowski J. (ed.), *Rosja. XX wiek. Od utopii komunistycznej do rzeczywistości globalistycznej*, transl. P. Burek, Wyd. Uniwersytetu Jagiellońskiego, Kraków 2004.



# Information Security Policy of Ukraine – Assumptions and Effectiveness

**ABSTRACT:** The paper presents the results of research on Ukraine’s information security, analysed from the perspective of its tenets, implementation and effectiveness. In this regard, the paper discusses aspects related to the development of conceptual tenets and preparation of a security strategy, as well as sectoral strategies and doctrines of information security and cybersecurity. The paper also contains an analysis of the institutional dimension of information security and actions taken by Ukraine in connection with the Russian aggression in terms of strategic communication and cybersecurity.

**KEYWORDS:** security policy, information policy, cybersecurity

## Introduction

Information security is becoming an increasingly important concept in the modern world and is among the key categories of national security interests. The technological revolution, digitisation and computerisation of states, as well as the dynamic development of mass media and the rising role and importance of social media, have affected the evolution and significance of these processes in the context of security. As a result, we now live in a world where aspects related to information, both in terms

of content and technology, play a key role in the functioning and security of states. These processes are important during peace but become even more crucial in times of danger, conflict and war. This is of particular significance given the current situation related to Russia's aggression against Ukraine. The purpose of this paper is, therefore, to present the results of research into Ukraine's information security policy, including its legal aspects, doctrinal assumptions and implementation during peacetime and during the war that began in early 2022.

As part of the research process, a hypothesis was formulated that Ukraine has increased its capabilities in terms of information resilience and the effectiveness of information security policy through implementing legislative, legal, organisational and technical means in recent years as a result of threats to its information security during this time. The research was based on the content analysis method, comparative method and historical method.

## Conceptual premises of information security

Concepts found in the normative document titled "Ukraine's information security strategy" (dated 28 December 2021) were used for this paper in terms of its definitional and conceptual aspects. According to the strategy, information security is "an integral part of Ukraine's national security, a way of ensuring the sovereignty of the state, its territorial integrity, democratic and constitutional governance, other vital interests of individuals, the society and the state – which guarantee constitutional rights and civil liberties, including the right to gather, store, use and distribute information and access reliable and objective information".<sup>1</sup> The above definition is complemented by the clarification of the concept of an "information threat", which is considered as "potential and actual phenomena, factors and tendencies related to the impact of information on the individual, the society and the state, which are present in the information sphere and whose purpose is to exert a negative influence aimed at preventing or hampering the achievement and pursuit of national interests".<sup>2</sup> Based on the above aspects and definitions, we can state that the information security of Ukraine has been given

---

<sup>1</sup> "Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»", *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/6852021-41069> (27.09.2022). See also: О.Д. Довгань, Т.Ю. Ткачук, "Система інформаційної безпеки України: онтологічні виміри", *Інформація і право*, vol. 1, no. 24 (2018), pp. 90–97.

<sup>2</sup> "Указ Президента України №685/2021..."

a broad definition that accounts for elements of a social, political, economic, technical and infrastructural nature.

## Ukraine's information security strategy

The above definition of Ukraine's information security is the product of many years of experience in this area, gained in recent years in which Ukraine was facing multiple challenges in this sphere due to the ongoing hybrid war.<sup>3</sup> The annexation of Crimea in 2014 and the subsequent conflict in the eastern oblasts of Ukraine, related to the activity of separatist entities supported by Russia, constituted a breakthrough in how Ukraine perceived security information and the threat posed by Russia in this area.<sup>4</sup> The evolution of threats in the sphere of information security and the need to take adequate action in response to them formed the basis of Ukraine's Strategy of National Security, adopted on 26 May 2015,<sup>5</sup> as well as Ukraine's Information Security (dated 25 February 2017).<sup>6</sup>

The hybrid war that raged in subsequent years confirmed the threats to information security were constantly rising. Ukraine reacted to these challenges on an ongoing basis and attempted to combat the threats in this area effectively. Experience from the confrontations that took place as part of the information war, and the resulting adaptation of the national security system in this sphere, also became the basis for a systemic analysis and update of strategic national security documents. Work aimed at

<sup>3</sup> Т. Жовтенко, "Гібридна війна: анатомія інструментарію й перемоги", *Democratic Initiatives*, 3.11.2022, [on-line:] <https://dif.org.ua/article/gibridna-viyna-anatomiya-instrumentariyu-y-peremogi> (27.09.2022); Т.О. Ісакова, "Пропаганда спрямована на розпалювання національної та міжнародної ворожнечі: проблеми визначення та протидії", *Аналітична записка*, no. 2, Серія «Інформаційні стратегії», NISS, 2.03.2015, [on-line:] <https://niss.gov.ua/doslidzhennya/informaciyni-strategii/propaganda-spryamovana-na-rozpalyuvannya-nacionalnoi-ta> (27.09.2022).

<sup>4</sup> See: M. L. Jaitner, "Russian Information Warfare: Lessons from Ukraine", in K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015, pp. 91–93.

<sup>5</sup> "Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року 'Про Стратегію національної безпеки України'", *Verkhovna Rada of Ukraine*, [on-line:] <https://zakon.rada.gov.ua/laws/show/392/2020#Text> (27.09.2022).

<sup>6</sup> "Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»", *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/472017-21374> (27.09.2022). See also: Т. Попова, "Що означає «Доктрина інформаційної безпеки України»?», *Radio Svoboda*, 27.02.2017, [on-line:] <https://www.radiosvoboda.org/a/28337376.html> (27.09.2022); "Доктрина інформаційної безпеки України – це лише декларація – експерти", *Radio Svoboda*, 27.02.2017, [on-line:] <https://www.radiosvoboda.org/a/28336852.html> (27.09.2022).

preparing new versions of these documents, taking into account the changed terms on which the hybrid war was being waged and rising threats in the information security area were constantly ongoing.<sup>7</sup>

Ukraine's new National Security Strategy was ultimately adopted on 14 September 2020. The document concerned broadly defined state security while accounting for challenges and threats in the sphere of information security. As far as this aspect was concerned, it was noted that given the circumstances, scale and importance of the information sector to national security, a special document concerning the specific area of information security had to be developed.<sup>8</sup> Work on the document continued in subsequent months, and ultimately on 28 December 2021, President Volodymyr Zelenskyy approved the *Strategy of Information Security of Ukraine*.<sup>9</sup>

The document points to the most critical aspects related to threats and challenges facing Ukraine in the sphere of information security. Guaranteeing Ukraine's security in this area was considered one of the state's most important tasks, given the severity of threats in this sphere, particularly in the context of the danger posed by Russia. The document stressed that Russia was pursuing a very aggressive policy in the sphere of information in respect of Ukraine, aimed at undermining the sovereignty and territorial integrity of the Ukrainian state. The objective of Ukraine's activity in the area of information security is to neutralise this aggressive policy pursued by the Russian Federation, as well as special operations related to information policy, aimed at weakening and undermining Ukraine's sovereignty and territorial integrity.<sup>10</sup>

---

<sup>7</sup> See also: "Аналіз Стратегії інформаційної безпеки в порівнянні з чинною Доктриною інформаційної безпеки", *Institute of Mass Information*, 29.04.2021, [on-line:] <https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoi-bezpeky-v-porivnyanni-z-chynnoyu-doktrynoyu-informatsijnoi-i38852> (27.09.2022).

<sup>8</sup> "Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року 'Про Стратегію національної безпеки України'", *Verkhovna Rada of Ukraine*, [on-line:] <https://zakon.rada.gov.ua/laws/show/392/2020#Text> (27.09.2022).

<sup>9</sup> "Указ Президента України №685/2021..."; See also: "Стратегію інформаційної безпеки-2025 прийнято: що зміниться у сфері цифрових прав?", *Digital Security Lab*, 18.01.2022 [on-line:] <https://dslua.org/publications/stratēhiiu-informatsijnoi-bezpeky-2025-pryyniato-shcho-zmynytisia-u-sferi-tsyfrovukh-prav/> (27.09.2022).

<sup>10</sup> "Указ Президента України №685/2021..."; "7 стратегічних цілей інформаційної безпеки України", *LexInform*, [on-line:] <https://lexinform.com.ua/zakonodavstvo/7-strategichnyh-tsiley-informatsijnoi-bezpeky-ukrayiny/> (27.09.2022).

## Analysis of threats in the area of information security

The evolution of considerations related to information security – both internationally and internally, as well as the perception of threats facing Ukraine – determined the division of dangers in this area. Taking into account the major aspects affecting key security information processes, the four following categories were considered the most important threats in the area of information:

- increase in the number of global disinformation campaigns;
- Russia's information policy (in respect of both Ukraine and other democratic states);
- an increase of the importance of social media in the context of impact factors and tools in the information space;
- insufficient level of development of competencies and skills in the context of the rapid development of information and digital technologies.<sup>11</sup>

Regarding threats in this international sphere, Ukraine treats information security as a challenge that constitutes a substantial global threat. Ongoing global disinformation campaigns pursued by authoritarian governments and radical groups aim to broadly impact, distort and manipulate social awareness. In the opinion of Ukrainian authorities, such actions are implemented by authoritarian countries on a widespread basis, which affects the democratic development of states and, from a broader perspective, international stability.<sup>12</sup>

In the context of the above challenges, the information policy and actions of the Russian Federation were considered a threat not only to the Ukrainian state, but to other democratic states as well. Based on experiences from activities pursued in recent years in respect of Ukraine, it was then found that Russia uses its special services and other dedicated structures to perform targeted operations and attacks against individual states. These attacks aim to influence internal public opinion and sow internal divisions among societies. The document, therefore, states that it is of paramount importance to counteract these operations and implement monitoring activities aimed at intercepting and eradicating intentional messages and disinformation.<sup>13</sup>

The use of social media is part of these activities. Their significance and use have risen sharply in recent years, which was determined by factors including globalisation

---

<sup>11</sup> “Указ Президента України №685/2021...”; В. Новицький, “Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах”, *Інформація і право*, vol. 1, no. 40 (2022), pp. 114–115.

<sup>12</sup> “Указ Президента України №685/2021...”

<sup>13</sup> *Ibidem*; “Президент увів у дію рішення РНБО про Стратегію інформаційної безпеки”, *Ukrinform*, 28.12.2021, [on-line:] <https://www.ukrinform.ua/rubric-polytics/3376906-prezident-uviv-u-diu-risenna-rnbo-pro-strategiu-informacijnoi-bezpeki.html> (27.09.2022).

and the COVID-19 pandemic. The specific nature of social media results in a significant increase in its importance for the social and political situation – both in terms of internal affairs of specific states as well as in the general context of global processes. Given the above, social media are a crucial tool in the modern security environment from the point of view of information and have extremely important effects from a security perspective.<sup>14</sup>

From the point of view of Ukraine's stance on threats, the above processes are correlated with the public perception of content and messages being communicated. Given the specific nature of contemporary media in terms of their availability, freedom and ease of conveying information and general accessibility, the strategy underlined the reduced social resilience to the content and narrative being communicated. Therefore, these considerations and processes constitute a significant threat given their potential for influencing and manipulating the entire society. They can significantly improve the effectiveness of information and psychological campaigns and the success of propaganda and disinformation and, as such, poses a significant threat to information security.<sup>15</sup>

## Internal dimension of threats in the information sphere

Given the list of threats in the sphere of information, analysing related processes and factors is of crucial importance from the perspective of Ukraine's circumstances and interests. The situation in this regard is affected by both systemic considerations and the heritage of Ukraine's social and political transformation processes and new phenomena and developments in this area. Due to this, Ukraine has delineated several key threats to national security in the sphere of information, which include the following processes:

- the information-related impact of the Russian Federation as an aggressor state on the Ukrainian people;
- Russia's domination in terms of information as an aggressor state in temporarily occupied areas of Ukraine;
- limited possibilities of reacting to and counteracting disinformation campaigns;
- the lack of an effective strategic communication system;
- imperfection in the regulation of relations in the sphere of information and protection of professional activities of journalists;

---

<sup>14</sup> “Указ Президента України №685/2021...”

<sup>15</sup> *Ibidem.*

- attempts to manipulate social consciousness in terms of European integration processes and Ukraine's Euro-Atlantic integration;
- limited access to information on the local level;
- insufficient level of information culture in society – in particular, in terms of susceptibility to manipulation and information influence.<sup>16</sup>

Ukraine pointed to information security on a national scale as one of the most important aspects of threats to its sovereignty and identity as a state. The Russian Federation was once again found to be the source of key threats in this sphere. Ukraine stressed that Russian intelligence services had been coordinating operations against Ukraine for some time, aimed at undermining its stability and internal security. The objective of these actions is to weaken Ukraine's national interests, sow division and conflict among its society, destabilise the social and political situation, eradicate Ukrainian national identity and ultimately bring about the end of Ukraine as a sovereign state. In this context, it's worth pointing out the actions taken and the current situation in terms of information security in areas occupied by the Russian Federation. Ukraine underlined that Russia had built a new information infrastructure in Crimea and was pursuing similar activities in the eastern oblasts of Ukraine. Apart from technical aspects, freedom of speech and civil liberties were restricted, and the activities of editing teams and journalists were under close supervision and control of authorities. As a result of these actions, the people living in these areas are cut off from any information disseminated by Ukraine and have access solely to narratives and propaganda content served by Russia. This situation poses a particular threat to Ukraine in the context of the state's communication with its citizens, supporting pro-Ukrainian attitudes and providing Ukrainians with information independent of the Russian authorities.<sup>17</sup>

The “destructive” propaganda and disinformation activities pursued by Russia on a comprehensive and full-scale basis constitute a key threat to the internal stability and security of the Ukrainian state in these two dimensions. By analysing the above threats, the tactics of which change depending on the current situation and social and political processes, Ukraine attempts to counteract them via various methods and

---

<sup>16</sup> *Ibidem*, “Зеленський затвердив Стратегію інформаційної безпеки України”, *Institute of Mass Information*, 29.12.2021, [on-line:] <https://imi.org.ua/news/zelenyskyj-zatverdyy-strategiyu-informatsijnoyi-bezpeky-ukrayiny-i43121> (27.09.2022).

<sup>17</sup> “Указ Президента України №685/2021...”; В. Новицький, *op. cit.*, pp. 114–115; See also: “Журналістика на території України в умовах гібридної війни: межі та можливості державного регулювання. Аналітична записка”, *NISS* [on-line:] <https://niss.gov.ua/doslidzhennya/informacijni-strategii/zhurnalistika-na-teritorii-ukraini-v-umovakh-gibridnoi-viyni> (27.09.2022).

activities. Authorities strive to adapt legal regulations and organisational solutions to the challenges facing them in this regard. However, as confirmed in the strategy, the analysis of the threats has still not led to the creation of comprehensive methods of counteracting and negating Russian “information aggression”. Ukraine has, therefore, implemented further plans and undertaken actions aimed at creating an effective system of strategic communication and preventing threats in the area of information that constitute a significant danger to the state’s stability and national security.<sup>18</sup>

Analysis of threats to internal information security shows that the situation in and functioning of the Ukrainian media market remains a significant problem in this regard. The structure of ownership and control of media by oligarch groups, limited potential for competition among media, as well as lack of independence of journalists from media owners are not conducive to the development and independence of media and affect the efficacy of actions undertaken to combat threats in the area of information security.<sup>19</sup>

The above is particularly true at the regional level, where media often remain dependent on local business structures and authorities. These circumstances are largely the product of the huge disproportions in the Ukraine media market. Huge disparities continue to exist between large cities and regional centres and smaller towns, where there is often a lack of information infrastructure and access to the internet. This has led to significant information exclusion of a large part of society and its dependence on local media.<sup>20</sup>

Of note is also that the above aspects of information policy were tied to Ukraine’s foreign and security policies, aimed at becoming part of the European Union and NATO. The strategy stresses that the majority of its citizens supports these two key objectives of Ukraine’s international policy. Given the strategic nature of this direction, Russia has been taking hostile action by manipulating and influencing Ukrainian citizens by disseminating untrue and stereotypical information on the EU and NATO. The purpose of this information is to destroy national consolidation and unity as to the direction of foreign and security policy and obstruct and subvert reforms being

---

<sup>18</sup> “Указ Президента України №685/2021...”; see also: “Президент затвердив Стратегію інформаційної безпеки: що передбачено”, *Jurliga*, 29.12.2021, [on-line:] [https://jurliga.ligazakon.net/news/208447\\_prezident-zatverdiv-strategyu-nformatsyno-bezpeki-shcho-peredbacheno](https://jurliga.ligazakon.net/news/208447_prezident-zatverdiv-strategyu-nformatsyno-bezpeki-shcho-peredbacheno) (27.09.2022).

<sup>19</sup> “Указ Президента України №685/2021...”

<sup>20</sup> *Ibidem*; “Міжнародний досвід впровадження медіаграмотності для окремих цільових груп: можливості для України”, *Niss*, 14.05.2019, [on-line:] <https://niss.gov.ua/doslidzhennya/informaciyini-strategii/mizhnarodniy-dosvid-vprovadzheniya-mediagramotnosti-dly> (27.09.2022).

implemented in the country in connection with its policy of integration with the EU and NATO.<sup>21</sup>

## Strategic objectives and directions of development of information security

Based on its analysis of considerations and threats related to the information area, Ukraine set seven strategic objectives, the achievement of which was to improve the situation in the diagnosed weak points of the information system. Implementing actions in these areas would also improve the resilience of the state and increase information security.<sup>22</sup> Based on the *Strategy of Information Security*, the following seven strategic objectives were set:

- Strategic objective No. 1: the objective concerns counteracting propaganda and disinformation, combating special operations in the area of information pursued by a hostile state, aimed at destroying constitutional governance, weakening the sovereignty and damaging the integrity of the Ukrainian state and eradicating Ukrainian independence. In this regard, Ukraine planned implementing a system of early warning and prevention of hybrid threats with particular attention placed on counteracting disinformation, propaganda, and information operations. Plans also included creating a mechanism of counteracting disinformation related to foreign policy and security of the Ukrainian state and its ongoing policy of European and Euro-Atlantic integration aimed at deepening Ukraine's cooperation with the EU and NATO;
- Strategic objective No. 2: the objective concerned strengthening Ukrainian identity and preparing and ensuring the comprehensive development of Ukrainian culture. This factor was determined as a key aspect in the context of building identity, a basis for the consolidation of the Ukrainian society and improving the national community;
- Strategic objective No. 3: the objective concerned activities aimed at improving the level of media culture and increasing the competences of citizens in the area of information. Actions in this aspect were directed mostly at improving social awareness to build resilience against propaganda, disinformation, destructive influences and manipulations forming part of hybrid activities pursued by the aggressor state;

<sup>21</sup> *Ibidem...*; В. Новицький, *op. cit.*, pp. 114–115.

<sup>22</sup> “Зеленський затвердив Стратегію...”; В. Новицький, *op. cit.*, pp. 114–115.

- Strategic objective No. 4: the objective concerned strengthening democratic processes and guaranteeing human rights in the area of information, freedom of speech and expressing one's views, and ensuring diversity of sources and access to verified, objective and reliable information. Strengthening journalistic work and guaranteeing the safety of those practising this profession, as well as freedom and independence of action while pursuing their duties;
- Strategic objective No. 5: the objective concerned a special form of Ukraine's information policy aimed at Ukrainian citizens living in occupied territories. The objective was described as "reintegration in terms of information" with the Ukrainian media space and own Ukrainian narratives addressed to these groups of citizens. Objectives in these areas were specified on a national and international scale. On the national scale, actions involved steps aimed at reaching citizens living in occupied areas with Ukrainian messages. On the international scale, the objective was to pursue consistent actions in respect of the international community, informing and reminding it of the status of Crimea and its occupation by Russia, as well as the occupation of the eastern oblasts of Ukraine;
- Strategic objective No. 6: the objective concerned actions aimed at implementing further changes and creating an effective system of strategic communication, with a focus on the key role of coordination of actions taken by authorities and structures responsible for information policy. Actions in this area were to result in strengthening cooperation between individual authorities and enabling them to counteract propaganda and disinformation effectively. It's worth noting that actions in this regard were focused on both internal and international circumstances and processes. Their goal was to counteract false Russian messaging concerning Ukraine and improve the state's positive image in the international arena;
- Strategic objective No. 7: the objective concerned actions aimed at developing and strengthening the society in the sphere of information and improving the culture of social dialogue. An integral part of these actions was to deepen and expand the public debate, improve the position of and funding for public broadcasters, expand modern information infrastructure and develop research into the information space, with a particular focus on the impact of new forms of mass media, social media, and online content on social processes and the functioning of societies.<sup>23</sup>

The strategic goals set were based mainly on a diagnosis of circumstances and challenges facing Ukraine in the information sphere. They were aimed primarily at improving the effectiveness of actions in the area of information security and the state's

---

<sup>23</sup> "Указ Президента України №685/2021..."; "7 стратегічних цілей інформаційної безпеки...".

resilience against internal and external threats. The Russian aggression on Ukraine cut these preparations short. Still, many of the implemented components contributed to increased effectiveness of actions taken by Ukraine in the information sphere and its narratives in the international arena concerning messaging around the Russian attack.

## Ukraine's cybersecurity

Cybersecurity is another key component of information security. From Ukraine's perspective, this sphere constitutes a very important part of national security due to frequent cyber-attacks on this country. As a result, on 15 March 2016, the then-President of Ukraine, Petro Poroshenko, adopted the first sectoral document, namely the Strategy of Cybersecurity of Ukraine.<sup>24</sup> After a few years, authorities decided to update the document<sup>25</sup> and, on 26 August 2021, President Volodymyr Zelenskyy approved the latest version of the Strategy of Cybersecurity of Ukraine.<sup>26</sup>

According to the document, the state's cybersecurity is one of the key priorities in Ukraine's national security system. It, therefore, stated that actions are needed in this area to improve the state's capabilities to counteract the cybernetic threats and attacks directed at Ukraine, particularly in the modern world, which has been seeing a rapid rise in the number of cyber threats, directly impacting a number of aspects of functioning and management of the country. The professional nature and nationalisation of cyberattacks are also of particular importance, which are carried out by special cybernetic units created as special forces forming part of the armed forces. As regards direct threats to Ukraine in this area, cybernetic threats were found to constitute "a possible arena of hostilities".<sup>27</sup>

The Russian Federation was again considered the source of Ukraine's cybernetic threats. Russia was found to be one of the greatest threats to cybersecurity, not only in

---

<sup>24</sup> "Указ Президента України №96/2016 Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/962016-19836> (27.09.2022).

<sup>25</sup> Д. Дубов, "Формуючи нову Стратегію кібербезпеки України: чи зможемо уникнути помилок першої спроби стратегування?", *NISS*, 27.01.2021, [on-line:] <https://niss.gov.ua/doslidzhennya/informaciyna-politika/formuyuchi-novu-strategiyu-kiberbezpeki-ukraini-chi-zmozhemo> (27.09.2022).

<sup>26</sup> "Указ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України», *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/4472021-40013> (27.09.2022).

<sup>27</sup> *Ibidem*; "Нова Стратегія кібербезпеки України", *LexInform*, [on-line:] <https://lexinform.com.ua/zakonodavstvo/nova-strategiya-kiberbezpeky-ukrayiny/> (27.09.2022).

Ukraine, but in other countries in the international arena as well, as Russia is carrying out special operations and attacks in cyberspace against the computer infrastructure of other countries, aiming to cripple them. Given the current technical considerations and processes in this area, from Ukraine's perspective, threats in the sphere of cybersecurity will continue to increase with the increase in the intensity of cyberattacks. Ukraine was particularly exposed to this threat and was planning on implementing actions aimed at improving its resilience and increasing the state's effectiveness in combating cybernetic security threats.<sup>28</sup>

This made it very important to determine the circumstances and specific nature of the operation of Ukraine's technological infrastructure and entire cybernetic system. Analysis in this regard was meant to ascertain the system's weak points and implement actions aimed at improving its effectiveness and resilience. Taking the above premises into account and based on the circumstances and threats present, major risk factors in the sphere of cybersecurity were found to (primarily) include Ukraine's high dependency on technological imports. Another vital consideration in this aspect was the dependency on foreign manufacturers and suppliers, as well as a lack of a system of technical supervision and control of the use of subsystems that could act as dual-use elements and generate a cyber threat. Other risk factors included the lack of modern legal regulations applicable to the dynamically changing sphere of cybersecurity and related threats, as well as the lack of a comprehensive system and organisation of national defence against cybernetic attacks on critical information infrastructure. The lack of adequate specialised units within central and local government institutions employing professionally prepared civil servants and experts responsible for cyber protection and security posed a significant challenge. The major reasons for the shortage of qualified personnel competent in cybersecurity matters in public institutions primarily included poor employment and salary conditions compared to those offered by the private sector.<sup>29</sup>

---

<sup>28</sup> “Указ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року...”. See also: “Щодо актуалізації використання кіберпростору як інструменту геополітичного суперництва. Аналітична записка”, *NISS*, 28.09.2016, [online:] <https://niss.gov.ua/doslidzhennya/informaciyni-strategii/schodo-aktualizacii-vikoristannya-kiberprostoru-yak> (27.09.2022).

<sup>29</sup> “Указ Президента України №447/2021 Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року...”.

## Information and the cybernetic dimension of the war

The Russian attack on Ukraine on 24 February 2022 led to a complete shift in the geopolitical situation – it changed international relations not only in Central and Eastern Europe, but in the wider global dimension. The information dimension was an important part of the aggression that began on that date and included cyberattacks which formed an integral part of the war. It bears stressing that starting from 24 February 2022, we have entered a new stage of information war and measures aimed at counteracting it in two aspects: narrative, propaganda and disinformation, as well as the cybersecurity aspect.

As already noted, one of the key challenges in information security (taking cyber threats into account) is ensuring the continued operation and coordination of individual state administration bodies. The operation of these structures gained particular importance and value after 24 February 2022. It completely changed the institutional dimension of information policy as most central and local government bodies became involved in the policy after hostilities broke out. However, it is worth stressing that actions aimed at improving the coordination of activity in this regard and creating a comprehensive system focused on improving the state's information security had already begun at an earlier date. The system was composed of state institutions and bodies, specialised agendas and public benefit institutions that collaborated with the public sectors.<sup>30</sup>

The Ukrainian *State Communication and Information Protection Service* was one of the more important structures in this system. The institution was created on 23 February 2006 and acted as a special authority (at the executive level) within the information security system that was tasked with coordinating activities, counteracting and neutralising threats and cyberattacks.<sup>31</sup> The structure also includes the specialised CERT-UA team, whose most important tasks include combating computer threats, gathering data for analysis and keeping a national register of cyber-incidents.<sup>32</sup> In con-

---

<sup>30</sup> Cf.: “Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні. Аналітична записка”, NISS, 19.12.2017, [on-line:] <https://niss.gov.ua/doslidzhennya/informaciyni-strategii/aktualni-pitannya-rozvitku-derzhavno-privatnoi-vzaemodii-u> (27.09.2022).

<sup>31</sup> “Закон України Про Державну службу спеціального зв'язку та захисту інформації України”, *Відомості Верховної Ради України*, no. 30, ст. 258 (2006), [on-line:] <https://zakon.rada.gov.ua/laws/show/3475-15#Text> (27.09.2022); “Державна служба спеціального зв'язку та захисту інформації України”, *State Service for Special Communications and Information Protection of Ukraine*, [on-line:] <https://cip.gov.ua/ua/statics/pro-derszhpeczv-yazku> (27.09.2022).

<sup>32</sup> *Про CERT-UA* [on-line:] <https://cert.gov.ua/about-us> (27.09.2022).

nection with the Russian aggression, on 28 July 2022, President Zelenskyy signed an act that amended several key documents concerning information security and cyber threats. The act also created a new structure – the *Centre for Active Counteraction of Aggression in Cyberspace*. Its task was the central coordination of efforts in cybersecurity and the prevention of ongoing acts of sabotage and attacks in this sphere.<sup>33</sup>

It is worth noting that under the *Act on the Basic Principles of Protection of Ukraine's Cybersecurity*, adopted on 5 October 2017, the *Ukrainian National Security and Defence Council* ensures the coordination of practical security tasks. A special structure, the *State Cybersecurity Coordination Centre*, operates as part of the council. It was created on 27 January 2016 and is responsible for coordinating the operations and functioning of entities tasked with ensuring the protection and security of the Ukrainian state in this sphere.<sup>34</sup> The main tasks of the centre include policy coordination, analysing the operation of entities and authorities active in the area of cybersecurity, predicting and counteracting cyber threats, preparing legislation proposals and practical solutions that improve security. The centre is also responsible for actions in the area of interoperability and uniformisation of Ukrainian solutions with NATO standards in the sphere of cybersecurity.<sup>35</sup>

Another important structure in the system is the *Strategic Communications Centre*, which forms part of the *Ministry of Culture and Information Policy*. Its major tasks include preventing propaganda and disinformation and counteracting the negative image of Ukraine in the international arena created by Russia. The centre's activities primarily focus on developing and strengthening strategic communication, counteraction and the promotion of the Ukrainian narrative in the international arena, which is aimed at expanding and deepening collaboration with foreign partners. Collaboration and coordination of actions – and exchange of experiences and information with countries who deal with similar threats and have similar involvements in the area of information

---

<sup>33</sup> “Закон України Про внесення змін до деяких законів України щодо забезпечення формування та реалізації державної політики у сфері активної протидії агресії у кіберпросторі”, *Verkhovna Rada of Ukraine*, [on-line:] <https://zakon.rada.gov.ua/laws/show/2470-20#n10> (27.09.2022); “В Україні може з'явитися центр протидії агресії РФ у кіберпросторі — законопроект”, *Sud.ua*, 4.07.2022 [on-line:] <https://www.sud.ua/ru/news/publication/242993-v-ukrayini-mozhe-zyavitisya-tsentr-protidiiy-agresiyi-rf-u-kiberprostori-zakonoproekt> (27.09.2022).

<sup>34</sup> “Закон України Про основні засади забезпечення кібербезпеки України”, *Відомості Верховної Ради*, no. 45, ст. 403 (2017), [on-line:] <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (27.09.2022).

<sup>35</sup> “Указ Президента України №242/2016 Про Національний координаційний центр кібербезпеки”, *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/2422016-20141> (27.09.2022).

security – also form an important part of this aspect.<sup>36</sup> A vital role, in this regard, is also played by individual structures that form part of the *Security Service of Ukraine*, which is active in the area of information security – in particular, when it comes to counteracting propaganda and disinformation, as well as intercepting cyberattacks and defending against them.

Collaboration within these structures, including coordinating the functioning of media and its messaging, is one of the key aspects of strategic communication during the ongoing war. Russia engaged in active operations in this regard and is pushing the narrative that the aggression is a “special operation” that was necessary due to several reasons (e.g., to fight Ukrainian fascists and nationalists who discriminate against the Russian-speaking population and illegally took power in Ukraine).

Regarding Ukraine’s information policy and strategic communication, it needs to be stressed that from the first days of the war, the Ukrainian authorities have engaged in cohesive actions and been presented a consistent narrative.

It is directed at its citizens, the international community and, at the beginning of the aggression, at Russians and Belarussians to encourage the citizens of these countries to actively oppose and protest against the attack on Ukraine. Announcements and appeals to stay calm, assurances that the Ukrainian army is ready to repulse the attack and defend its country, and calls to adopt patriotic attitudes and engage in civil resistance were extremely important from the perspective of effectiveness and defence of the country. In the international dimension, the main narrative is focused on counteracting Russian propaganda by spotlighting Russia’s aggression on a sovereign and independent country, constituting a total violation of international standards and laws and the world order created after World War II. Ukraine also stresses that the attack was completely unfounded and actively informs the international community about the atrocities of war, attacks on civil infrastructure and defenceless people – and genocide taking place in areas occupied by Russian forces – by calling on the international community to impose sanctions and limit its cooperation with the aggressor. It needs to be stressed that President Volodymyr Zelenskyy has become a key figure when it comes to strategic communication. His decision to remain in Kyiv in the first days of the war was an important aspect that helped keep the morale of Ukrainian soldiers up and foil Russia’s plans of a quick conquest of Ukraine.<sup>37</sup>

---

<sup>36</sup> “Центр стратегічних комунікацій”, *Centre for Strategic Communication*, [on-line:] <https://spravdi.gov.ua/pro-nas> (27.09.2022).

<sup>37</sup> А.М. Дунер, М. Пічowska, “Ukraine’s Wartime Information Strategy”, *Bulletin PISM*, 4.04.2022. See also: “Бій за Африку: як українська дипломатія розширює горизонти та бореться з впливом росії на континенті”, *Democratic Initiatives*, 1.11.2022, [on-line:] <https://dif.org.ua/article/>

As regards the cybernetic dimension of the ongoing war, of particular note is that cyberattacks against Ukraine intensified in the months leading up to the aggression. The attacks were primarily aimed at strategic state management sectors and critical infrastructure systems. On the eve of the Russian aggression, one of the largest cyberattacks in Ukraine's history took place. A mass DDoS (distributed denial-of-service) attack was launched against websites of the Ukrainian government and the online system of one of Ukraine's largest banks. Another cyberattack took place on the eve of the attack and was again aimed against government websites, critical infrastructure and the *Viasat* satellite network. The attacks continued in subsequent weeks and were most frequent in the first three months of the aggression. Due to these risks, the Ukrainian authorities decided to transfer their data to servers abroad and enlisted the services of global commercial companies for this purpose. In subsequent weeks of the war, several dozen central government bodies decided to follow suit and transfer databases of key importance abroad from the perspective of national security.<sup>38</sup>

As previously noted, an important task is coordinating actions by several bodies responsible for cybersecurity, including specialised structures of the *Security Service of Ukraine* – which is responsible for counteracting disinformation and propaganda, as well as coordinating defence against cyberattacks.<sup>39</sup> It should be noted that these are unseen actions that take place in the computer world, but they constitute an integral part of the ongoing war. Ukrainian experts react to threats in this sphere on an ongoing basis. According to the *Department of Cybersecurity of the Security Service of Ukraine*, between the start of the aggression and November 2022, Russia launched over 3,500 cyberattacks against Ukraine, with over ten attacks occurring daily.<sup>40</sup>

---

biy-za-afriku-yak-ukrainska-diplomatiya-rozshiryue-gorizonti-ta-boretsya-z-vplivom-rosii-na-kontinenti?fbclid=IwAR1pqtJpEnhJKlaC-INxYGQzDchhy98vVBJ-7UnvtHv\_E4OQY4OgOW88OFQ (27.09.2022).

<sup>38</sup> Д. Петровський, “Перша світова кібервійна”, *Unian*, 3.10.2022, [on-line:] <https://www.unian.ua/techno/persha-svitova-kiberviyuna-yak-ukrajina-boretsya-na-drugomu-fronti-11998566.html> (28.09.2022); “Кібератака в Україні 15 лютого була найбільшою в історії держави: в Кабміні назвали вартість”, *Unian*, 16.02.2022, [on-line:] <https://www.unian.ua/techno/communications/kiberataka-v-ukrajini-15-lyutogo-bula-naybilshoyu-v-istoriji-derzhavi-v-kabmini-nazvali-vartist-11706571.html> (28.09.2022).

<sup>39</sup> “СБУ ліквідувала у Дніпрі ворожу ботоферму, яка створила майже 10 тис. фейкових акаунтів для «розгону» кремлівської пропаганди в ЄС”, *Security Service of Ukraine*, 20.10.2022, [on-line:] <https://ssu.gov.ua/novyny/sbu-likvidovala-u-dnipri-vorozhu-botofermu-yaka-stvoryla-maizhe-10-tys-feikovykh-akauntiv-dlia-rozghonu-kremlivskoi-propahandy-v-yes> (28.09.2022).

<sup>40</sup> “рф щодня здійснює понад 10 кібератак на стратегічні об’єкти України, – керівник Департаменту кібербезпеки СБУ”, *Security Service of Ukraine*, 9.11.2022, [on-line:] <https://ssu.gov.ua/novyny/rf-shchodnia-zdiisniue-ponad-10-kiberatak-na-stratehichni-objekty-ukrainy-kerivnyk-departamentu-kiberbezpeky-sbu> (28.09.2022).

As previously noted, the activities of central government authorities in the area of information security were complemented by actions taken by structures on the regional level and close cooperation with public benefit institutions and individual specialists. These entities demonstrated significant flexibility in action and efficiency in combating information and cybernetic threats in information security. Cooperation, in this regard, intensified following Russia's aggression, and the mutual exchange of experiences between the non-governmental sector and state structures impacted the effectiveness of crisis management in the area of information security.

It needs to be stressed that many governmental and grassroots initiatives aimed at preventing hacking attacks appeared in connection with the outbreak of the war. One of the more effective initiatives was the creation of an 'IT army' by the *Ministry of Digitisation of Ukraine* – the product of combined forces and efforts of companies representing various strategic sectors of the state, IT experts and volunteers interested in supporting this type of activities who received adequate training. According to available information, the IT army may number up to 200,000 specialists actively participating in cyber war. One of their more effective and widely publicised achievements was their hacking of *Wagner Group's* servers and identification of those of its members who participated in the aggression on Ukraine. Reports in the media also indicate that in late August and early September 2022, the group attacked and disabled over 2,400 Russian portals and websites (including such powerful ones as *Gazprombank, KreditBank Moscow, Sovcombank, Rambler, Gazeta.ru. MK*).<sup>41</sup> It, therefore, needs to be stressed that Ukrainians do not limit themselves exclusively to defence, but also engage in active counteraction by forcing the attackers to defend and limit their offensive action. This translates into a reduced number of attacks during this time, which points to the effectiveness of the action taken by Ukrainians.<sup>42</sup>

---

<sup>41</sup> Д. Петровський, *op. cit.*

<sup>42</sup> В. Орлова, "Как работает IT-армия Украины и какие победы уже на ее счету. Объяснение Федорова", *RBC*, 27.04.2022, [on-line:] <https://www.rbc.ua/rus/news/rabotaet-it-armiya-ukrainy-kakie-pobedy-schetu-1651046717.html>; "IT-армія України: чим вона займається та які перемоги вже на її рахунку", *Unian*, 27.04.2022, [on-line:] <https://www.unian.ua/techno/communications/it-armiya-ukrajini-chim-vona-zaymayetsya-ta-yaki-peremogi-vzhe-na-jiji-rahunku-11803026.html> (28.09.2022); "Україна веде активний контрнаступ на кіберфронті – Ілля Вітюк", *Security Service of Ukraine*, 17.10.2022, [on-line:] <https://ssu.gov.ua/novyny/ukraina-vede-aktyvnyi-kontrnastup-na-kiberfronti-illia-vitiuk> (28.09.2022).

## Summary

Based on the research process and verification of the formulated research hypothesis we can conclude that Ukraine has significantly increased its effectiveness and capabilities in terms of information resilience and efficiency of security policy. The process was impacted by the implementation of comprehensive decisions and actions in respect of individual aspects of information security, such as legislative and legal actions and improvement of information infrastructure. The annexation of Crimea in 2014 and the subsequent conflict in the eastern oblasts of Ukraine constituted a breakthrough in the formation of Ukraine's information security policy. The events marked a turning point at which Ukraine was forced to react to the propaganda and disinformation activities that Russia engaged in on a mass scale, both internally in respect of Ukrainian citizens, and in respect of the wider international community. It was at this stage that Ukrainian authorities made further key decisions aimed at improving their information security and counteracting the increasing threat posed by Russia in this area. This was reflected in the successive adoption of security strategies and specialised documents focusing directly on information security and cybersecurity. Ukraine followed the implementation of legal regulations with practical actions aimed at improving its information security and counteracting threats in this area. After Russia began its aggression in early 2022, Ukraine was therefore able to build on its experiences of the past few years and showed good effectiveness in this area. Ukraine has been able to effectively counteract and combat propaganda and disinformation, and has been taking actions in the area of strategic communication in order to strengthen its own narrative on the Russian aggression and the ongoing war on the international arena. Confrontation in the cyberspace is an integral part of the conflict and Ukraine has been waging war effectively in this area as well, largely based on its experiences of the past few years.

In summary, we can conclude that the information security pursued by Ukraine in recent years, despite its many flaws and issues, has allowed the country to gain experience and prepare for defence, which has been extremely important and efficiently utilised in the course of the current aggression. The ongoing war has again confirmed that in the context of both strategic communication and cybersecurity, aspects related to information have an extremely important role to play in the modern society, both in terms of resilience of states and tools used for waging war. Further analysis of the ongoing war in terms of its information aspect are therefore required and this area of national security and defence must continue to be improved, taking into account

Ukraine's experiences and conclusions in terms of the ongoing fight in the area of strategic communication and cybersecurity.

## References

- “7 strategičnih cilej informacijnoј bezpeki Ukraїni” [“7 стратегічних цілей інформаційної безпеки України”], *LexInform*, [on-line:] <https://lexinform.com.ua/zakonodavstvo/7-strategichnyh-tsilej-informatsijnoyi-bezpeky-ukrayiny/>.
- “Aktual'ni pitannâ rozvitku deržavno-privatnoј vzaємодії u sferi zabezpečennâ kiberbezpeki v Ukraїni. Analitična zapiska” [“Актуальні питання розвитку державно-приватної взаємодії у сфері забезпечення кібербезпеки в Україні. Аналітична записка”], *NISS*, 19.12.2017, [on-line:] <https://niss.gov.ua/doslidzhennya/informacijni-strategii/aktualni-pitannya-rozvitku-derzhavno-privatnoi-vzaemodii-u>.
- “Analiz Strategii informacijnoј bezpeki v porivnânni z činnoū Doktrinoū informacijnoј bezpeki” [“Аналіз Стратегії інформаційної безпеки в порівнянні з чинною Доктриною інформаційної безпеки”], *Institute of Mass Information*, 29.04.2021, [on-line:] <https://imi.org.ua/monitorings/analiz-strategiyi-informatsijnoyi-bezpeky-v-porivnyanni-z-čynnoyu-doktrynoyu-informatsijnoyi-i38852>.
- “Bij za Afriku: âk ukraїns'ka diplomatîâ rozširûe gorizonti ta boreťsâ z vplivom rosii na kontinenti” [“Бій за Африку: як українська дипломатія розширює горизонти та бореться з впливом росії на континенті”], *Democratic Initiatives*, 1.11.2022, [on-line:] [https://dif.org.ua/article/bij-za-afriku-yak-ukraїnska-diplomatiya-rozshiruyegorizonti-ta-boretsya-z-vplivom-rosii-na-kontinenti?fbclid=IwAR1pqtJpEnhJKlaC-INxYGQzDchhy98vVBJ-7UnvtHv\\_E4OQY4OgOW88OFQ](https://dif.org.ua/article/bij-za-afriku-yak-ukraїnska-diplomatiya-rozshiruyegorizonti-ta-boretsya-z-vplivom-rosii-na-kontinenti?fbclid=IwAR1pqtJpEnhJKlaC-INxYGQzDchhy98vVBJ-7UnvtHv_E4OQY4OgOW88OFQ).
- “Centr strategičnih komunikacij” [“Центр стратегічних комунікацій”], *Centre for Strategic Communication*, [on-line:] <https://spravdi.gov.ua/pro-nas>.
- “Deržavna služba special'nogo зв'язku ta zahistu informaciji Ukraїni” [“Державна служба спеціального зв'язку та захисту інформації України”], *State Service for Special Communications and Information Protection of Ukraine*, 1.06.2022, [on-line:] <https://cip.gov.ua/ua/statics/pro-derszhpeczv-yazku>.
- “Doktrina informacijnoј bezpeki Ukraїni – ce liše deklaraciâ – eksperti” [“Доктрина інформаційної безпеки України – це лише декларація – експерти”], *Radio Svoboda*, 27.02.2017, [on-line:] <https://www.radiosvoboda.org/a/28336852.html>.
- Dovhan O.D., Tkačuk T.Ū., “Sistema informacijnoј bezpeki Ukraїni: ontologični vimiri”, *Інформація і право* [Довгань О.Д., Ткачук Т.Ю., “Система інформаційної безпеки України: онтологічні виміри”, *Інформація і право*, vol. 1, no. 24 (2018), pp. 90–97.
- Dubov D., “Formuïci novu Strategii kiberbezpeki Ukraїni: či zmožemo uniknuti pomilok peršoi sprobi strateguvannâ?” [Дубов Д., “Формуючи нову Стратегію кібербезпеки України: чи зможемо уникнути помилок першої спроби стратегування?”], *NISS*, 27.01.2021, [on-line:] <https://niss.gov.ua/doslidzhennya/informacijna-politika/formuuyuchi-novu-strategiyu-kiberbezpeki-ukraini-chi-zmozhemo>.

- Dyner A.M., Piechowska M., “Ukraine’s Wartime Information Strategy”, *Bulletin PISM*, 4.04.2022, <https://doi.org/10.1177/009286157000400119>.
- Isakova T.O., “Propaganda sprámovana na rozpalúvannâ nacional’noï ta mižnacional’noï vorožneçi: problemi viznačennâ ta protidii”, *Analična zapiska*, no. 2, Seriâ «Înformacijni strategii» [Isakova T.O., “Пропаганда спрямована на розпалювання національної та міжнаціональної ворожнечі: проблеми визначення та протидії”, *Аналітична записка*, no. 2, Серія «Інформаційні стратегії»], *NISS*, 2.03.2015, [on-line:] <https://niss.gov.ua/doslidzhennya/informacijni-strategii/propaganda-spryamovana-na-rozpaljuvannya-nacionalnoi-ta>.
- “IT-armiâ Ukraïni: čim вона займаєт’ся та âki peremogi vže na її rahunku” [“ІТ-армія України: чим вона займається та які перемоги вже на її рахунок”], *Unian*, 27.04.2022, [on-line:] <https://www.unian.ua/techno/communications/it-armiya-ukrajini-chim-vo-na-zaumayetsya-ta-yaki-peremogi-vzhe-na-ji-rahunku-11803026.html>.
- Jaitner M.L., “Russian Information Warfare: Lessons from Ukraine”, in K. Geers (ed.), *Cyber War in Perspective: Russian Aggression against Ukraine*, NATO CCD COE Publications, Tallinn 2015.
- “Kiberataka v Ukraïni 15 lûtogo bula najbil’šoû v istorii deržavi: v Kabmini nazvali vartist” [“Кібератака в Україні 15 лютого була найбільшою в історії держави: в Кабміні назвали вартість”], *Unian*, 16.02.2022, [on-line:] <https://www.unian.ua/techno/communications/kiberataka-v-ukrajini-15-lyutogo-bula-naybilshoyu-v-istoriji-derzhavi-v-kabmini-nazvali-vartist-11706571.html>.
- “Mižnarodnij dosvid vprovadžennâ mediagramotnosti dlâ okremih ciľovih grup: možlivosti dlâ Ukraïni” [“Міжнародний досвід впровадження медіаграмотності для окремих цільових груп: можливості для України”], *NISS*, 14.05.2019, [on-line:] <https://niss.gov.ua/doslidzhennya/informacijni-strategii/mizhnarodnij-dosvid-vprovadzheniya-mediagramotnosti-dlya>.
- “Nova Strategiâ kiberbezpeki Ukraïni” [„Нова Стратегія кібербезпеки України”], *LexInform*, [on-line:] <https://lexinform.com.ua/zakonodavstvo/nova-strategiya-kiberbezpeky-ukrayiny/>.
- Novytskyi V., “Strategični zasadi zabezpečennâ informacijnoï bezpeki v sučasnih umovah”, *Înformaciâ i pravo* [Новицький В., “Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах”, *Інформація і право*], vol. 1, no. 40 (2022), pp. 114–115.
- Orlova V., “Kak rabotaet IT-armiâ Ukrainy i kakie pobedy uže na ee ščetu. Ob’âsnenie Fedorova” [Орлова В., “Как работает IT-армия Украины и какие победы уже на ее счету. Объяснение Федорова”], *RBC*, 27.04.2022, [on-line:] <https://www.rbc.ua/rus/news/rabotaet-it-armiya-ukrainy-kakie-pobedy-schetu-1651046717.html>.
- Petrovsky D., “Perša svitova kibervijna” [Петровський Д., “Перша світова кібервійна”], *Unian*, 3.10.2022, [on-line:] <https://www.unian.ua/techno/persha-svitova-kiberviynayak-ukrajina-boretsya-na-drugomu-fronti-11998566.html>.
- Porova T., “Šo označae «Doktrina informacijnoï bezpeki Ukraïni?»” [Попова Т., “Що означає «Доктрина інформаційної безпеки України?»”], *Radio Svoboda*, 28.02.2017, [on-line:] <https://www.radiosvoboda.org/a/28337376.html>.
- “Prezident uviv u diû rišennâ RNBO pro Strategiû informacijnoï bezpeki” [“Президент увів у дію рішення РНБО про Стратегію інформаційної безпеки”], *Ukrinform*, 28.12.2021,

- [on-line:] <https://www.ukrinform.ua/rubric-politics/3376906-prezident-uviv-u-diu-risenna-rnbo-pro-strategiu-informacijnoi-bezpeki.html>.
- “Prezident zatverdiv Strategiju informacijnoi bezpeki: šo prevedbачeno” [“Президент затвердив Стратегию информационной безопасности: что prevedbачено”], *Jurliga*, 29.12.2021, [on-line:] [https://jurliga.ligazakon.net/news/208447\\_prezident-zatverdiv-strategiu-nformatsyno-bezpeki-shcho-peredbачeno](https://jurliga.ligazakon.net/news/208447_prezident-zatverdiv-strategiu-nformatsyno-bezpeki-shcho-peredbачeno).
- “rf šodnâ zdijsnûe ponad 10 kiberatak na strategični oběkti Ukraïni, – kerivnik Departamentu kiberbezpeki SBU” [“рф щодня здійснює понад 10 кібератак на стратегічні об'єкти Украïни, – керівник Департаменту кібербезпеки СБУ”], *Security Service of Ukraine*, 9.11.2022, [on-line:] <https://ssu.gov.ua/novyny/rf-shchodnia-zdiisniue-ponad-10-kiberatak-na-stratehichni-objekty-ukrainy-kerivnyk-departamentu-kiberbezpeky-sbu>.
- “SBU likvidovala u Dnipri vorožu botofermu, âka stvorila majže 10 tis. fejkovih akauntiv dlâ «rozgonu» kremlivs'koï propagandi v ÊS” [“СБУ ліквідувала у Дніпрі ворожу ботоферму, яка створила майже 10 тис. фейкових акаунтів для «розгону» кремлівської пропаганди в ЄС”], *Security Service of Ukraine*, 20.10.2022, [on-line:] <https://ssu.gov.ua/novyny/sbu-likvidovala-u-dnipri-vorozhu-botofermu-yaka-stvorila-maizhe-10-tys-feikovykh-akauntiv-dlia-rozghonu-kremlivskoi-propahandy-v-yes>.
- “Šodo aktualizacii vikoristannâ kiberprostoru âk instrumentu geopolitичного superництва. Analitična zapiska” [“Щодо актуалізації використання кіберпростору як інструменту геополітичного суперництва. Аналітична записка”], *NISS*, 28.09.2016, [on-line:] <https://niss.gov.ua/doslidzhennya/informacijni-strategii/schodo-aktualizacii-vikoristannya-kiberprostoru-yak>.
- “Strategiju informacijnoi bezpeki-2025 prijnâto: šo zmnit'sâ u sferi cifrovih prav?” [“Стратегию информационной безопасности-2025 прийнято: що зміниться у сфері цифрових прав?”], *Digital Security Lab*, 18.01.2022, [on-line:] <https://dslua.org/publications/strategiiu-informatsijnoi-bezpeky-2025-pryjniato-shcho-zminytsia-u-sferi-tsyfrovykh-prav/>.
- “Ukaz Prezidenta Ukraïni №242/2016 Pro Nacional'nij koordinacijnij centr kiberbezpeki” [“Указ Президента Украïни №242/2016 Про Національний координаційний центр кібербезпеки”], *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/2422016-20141>.
- “Ukaz Prezidenta Ukraïni №447/2021 Pro rišennâ Radi nacional'noï bezpeki i oboroni Ukraïni від 14 travnâ 2021 roku «Pro Strategiju kiberbezpeki Ukraïni»” [“Указ Президента Украïни №447/2021 Про рішення Ради національної безпеки і оборони Украïни від 14 травня 2021 року «Про Стратегию кібербезпеки Украïни»”], *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/4472021-40013>.
- “Ukaz Prezidenta Ukraïni №47/2017 Pro rišennâ Radi nacional'noï bezpeki i oboroni Ukraïni від 29 grudnâ 2016 roku «Pro Doktrinu informacijnoi bezpeki Ukraïni»” [“Указ Президента Украïни №47/2017 Про рішення Ради національної безпеки і оборони Украïни від 29 грудня 2016 року «Про Доктрину інформаційної безпеки Украïни»”], *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/472017-21374>.
- “Ukaz Prezidenta Ukraïni №685/2021 Pro rišennâ Radi nacional'noï bezpeki i oboroni Ukraïni від 15 žovtnâ 2021 roku «Pro Strategiju informacijnoi bezpeki»” [“Указ Президента Украïни №685/2021 Про рішення Ради національної безпеки і оборони Украïни від

- 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»], *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/6852021-41069>.
- “Ukaz Prezidenta Ukraïni №96/2016 Pro rišennâ Radi nacional’noi bezpeki i oboroni Ukraïni від 27 січня 2016 року «Про Стратегію кібербезпеки Украïни»” [“Указ Президента Украïни №96/2016 Про рішення Ради національної безпеки і оборони Украïни від 27 січня 2016 року «Про Стратегію кібербезпеки Украïни»”], *President of Ukraine: Official website*, [on-line:] <https://www.president.gov.ua/documents/962016-19836>.
- “Ukaz Prezidenta Ukraïni Pro rišennâ Radi nacional’noi bezpeki i oboroni Ukraïni від 14 вересня 2020 року ‘Pro Strategію nacional’noi bezpeki Ukraïni’” [“Указ Президента Украïни Про рішення Ради національної безпеки і оборони Украïни від 14 вересня 2020 року ‘Про Стратегію національної безпеки Украïни’”], *Verkhovna Rada of Ukraine*, [on-line:] <https://zakon.rada.gov.ua/laws/show/392/2020#Text>.
- “Ukaz Prezidenta Ukraïni Pro rišennâ Radi nacional’noi bezpeki i oboroni Ukraïni від 14 вересня 2020 року ‘Pro Strategію nacional’noi bezpeki Ukraïni’” [“Указ Президента Украïни Про рішення Ради національної безпеки і оборони Украïни від 14 вересня 2020 року ‘Про Стратегію національної безпеки Украïни’”], *Verkhovna Rada of Ukraine*, [on-line:] <https://zakon.rada.gov.ua/laws/show/392/2020#Text>.
- “Ukraïna vede aktivnij kontrnastup na kiberfronti – Illâ Vitûk” [“Украïна веде активний контрнаступ на кіберфронті – Ілля Вітук”], *Security Service of Ukraine*, 17.10.2022, [on-line:] <https://ssu.gov.ua/novyny/ukraina-vede-aktyvnyi-kontrnastup-na-kiberfronti-illia-vitiuk>.
- “V Ukraïni može z’âvitisâ centr protidii agresii RF u kiberprostori – zakonoproekt” [“В Украïни може з’явитися центр протидії агресії РФ у кіберпросторі – законопроект”], *Sud.ua*, 4.07.2022, [on-line:] <https://www.sud.ua/ru/news/publication/242993-v-ukrayini-mozhe-z-yavitisya-tsentr-protidii-agresiyi-rf-u-kiberprostori-zakonoproekt>.
- “Zakon Ukraïni Pro Deržavnu službu special’nogo зв’язku ta zahistu informacii Ukraïni”, *Vidomosti Verhovnoi Radi Ukraïni* [“Закон Украïни Про Державну службу спеціального зв’язку та захисту інформації Украïни”, *Vidomosti Verhovnoi Radi Ukraïni*], no. 30, ст. 258 (2006), [on-line:] <https://zakon.rada.gov.ua/laws/show/3475-15#Text>.
- “Zakon Ukraïni Pro osnovni zasady zabezpečennâ kiberbezpeki Ukraïni”, *Vidomosti Verhovnoi Radi* [“Закон Украïни Про основні засади забезпечення кібербезпеки Украïни”], *Vidomosti Verhovnoi Radi*, no. 45, ст. 403 (2017), [on-line:] <https://zakon.rada.gov.ua/laws/show/2163-19#Text>.
- “Zelens’kij zatverdiv Strategію informacijnoi bezpeki Ukraïni” [“Зеленський затвердив Стратегію інформаційної безпеки Украïни”], *Institute of Mass Information*, 29.12.2021, [on-line:] <https://imi.org.ua/news/zelenskyj-zatverdvy-strategiyu-informatsijnoyi-bezpeky-ukrayiny-i43121>.
- Zhovtenko T., “Gibridna vijnâ: anatomіâ instrumentariu j peremogi” [“Гібридна війна: анатомія інструментарію й перемоги”], *Democratic Initiatives*, 3.11.2022, [on-line:] <https://dif.org.ua/article/gibridna-vijna-anatomiya-instrumentariyu-y-peremogi>.
- “Žurnalistika na teritorii Ukraïni v umovah gibridnoi vijnі: meži ta možlivosti deržavnogo reguluvannâ. Analitična zapiska” [“Журналистика на території Украïни в умовах гібридної війни: межі та можливості державного регулювання. Аналітична записка” [“Закон Украïни Про внесення змін до деяких законів Украïни щодо забезпечення формування та реалізації державної політики

у сфері активної протидії агресії у кіберпросторі”], *Verkhovna Rada of Ukraine*, 28.07.2022, [on-line:] <https://zakon.rada.gov.ua/laws/show/2470-20#n10>.

“Журналістика на території України в умовах гібридної війни: межі та можливості державного регулювання. Аналітична записка”, *NISS*, [on-line:] <https://niss.gov.ua/doslidzhennya/informaciyni-strategii/zhurnalistika-na-teritorii-ukraini-v-umovakh-gibridnoi-viyni>.



## Index of names

- Adler-Nissen Rebecca 29  
al-Assad Bashar 70  
Antosiewicz Maciej 15  
Apuzzo Matt 47  
Arendt Hannah 92
- Bäcker Roman 92  
Bajor Piotr 7, 99  
Bastos Marco T. 10  
Bernaczyk Michał 21  
Bernatskyi Bohdan 38  
Bilal Arsalan 11  
Borrell Josep 74  
Bryjka Filip 42, 47  
Brzeziński (Brzeziński) Zbigniew 86–87  
Budzisz Marek 91  
Bukowski Maciej 37  
Burek Paweł 89
- Castells Manuel 12–13  
Ciuriak Dan 16  
Clegg Nick 23, 28  
Cohen Saul B. 85–87  
Conley Heather A. 90  
Coutau-Bégarie Hervé 68  
Czeszejko Stanisław 68
- Danek Magdalena 9, 21–22  
Davis Julia 16  
Diec Joachim 87–88  
Dijk Jan van 10  
Domańska Maria 90  
Dovhan Oleksandr D. (Довгань Олександр Д.) 100
- Dubov Dmytro (Дубов Дмитро) 109  
Dugin Aleksandr (Alexander) 37, 87  
Durov Pavel 73  
Duszczyk Maciej 37  
Dyner Anna Maria 113
- Eberhardt Piotr 87  
Easton David 36  
Eddy Melissa 46  
Ellul Jacques 72
- Fedorov Mykhailo 23, 77  
Fijałkowski Łukasz  
Foucault Michel 13  
Foxall Andrew 70  
Fraser Małgorzata 40
- Gąsior Tomasz 21  
Geers Kenneth 101  
Gerasimov Valery 11  
Gigitashvili Givi 19  
Glavin Terry 46  
Golovchenko Yevgeniy 29  
Grodzki Radosław 71  
Guess Andrew 10  
Gulczyński Michał 43
- Hartmann Mareike 29  
Haugen Francis 14  
Hughes Chris 15
- Irisova Olga 70  
Isakova T.O. (Исакова Т.О.) 101

- Jaitner Margarita L. 101  
Janczak Józef 68  
Jedliński Jakub 13  
Jungherr Andreas 30
- Kaźmierczak Danuta 70  
Kemp Simon 13  
Khodorkovsky Mikhail 89  
King Martin Luther 78  
Kissinger Henry 14–15  
Komendant Tadeusz 13  
Konieczny Jacek 10  
Kosienkowski Marcin 84  
Kozak Dmitry 91  
Kravtsov Sergei 91  
Kruglashov Anatoliy 71
- Lavrov Sergei 91  
Lenin Vladimir (Vladimir Ilyich Ulyanov) 95  
Le Pen Marine 38, 42  
Lewicki Stanisław 58  
Lim Cristiano 14  
Lim Zheng Wei 21  
Ling Richard 21  
Lohsen Andrew 90
- Łojkowska Małgorzata 89
- Maciejak Maciej 71  
Maćkowiak Anna 93  
Mahda Yevhen (Магда Євген) 54  
Marek Michał 54  
Marody Mirosława 12  
McKay Spencer 15  
McSweeney Sinéad 26  
Medvedev Dmitry 17  
Mercea Dan 10  
Merrill Jeremy B. 14  
Misiuna Jan 21  
Musk Elon 77
- Navalny Alexei 25, 89  
Nimmo Ben 18–19  
Nitszke Agnieszka 35
- Novytskyi V. (Новицький В.) 103, 105, 107  
Nyhan Brendan 10
- Obama Barack 15  
Oleksy Piotr 84  
O'Loughlin John 91  
Oremus Will 14  
Orlova V. (Орлова В.) 115
- Panarin Igor 87  
Parfitt Tom 70  
Petrovsky Dmytro (Петровський Дмитро) 114–115  
Philotheus of Pskov 88  
Pikta Swietłana 58  
Piechowska Maria 113  
Pieciukaitis Aurimas L. 60  
Piłsudski Józef 61  
Piskorski Mateusz 58  
Połowaniuk Marcin 16  
Popova Tatiana (Попова Тетяна) 101  
Poroshenko Petro 73, 109  
Potulski Jakub 87  
Primakov Andrei 90  
Putin Vladimir 27, 37, 70, 73, 75, 78, 83–84, 89–95  
Putnam Robert 10  
Puto Kaja 73
- Radzik Ryszard 88–89  
Rak Joanna 93  
Reczkowski Robert 40  
Reifler Jason 10  
Rocha Yasmim Mendes 10  
Rogoża Jadwiga 89  
Ruy Donatienne 39
- Saakashvili Mikhail 71  
Sadura Przemysław 10  
Salvini Matteo 38  
Sartori Giovanni 42  
Saurwein Florian 20  
Schroeder Ralph 30  
Schwartau Winn 68

- Scott Mark 14, 46  
Sechin Igor 73  
Serdyukov Anatoly 72  
Serowaniec Maciej 21  
Shoygu Sergei 72  
Shvydiuk Sergii 71  
Smith Brad 69  
Sokała Witold 76  
Spencer-Smith Charlotte 20  
Stalin Joseph Vissarionovich (Ioseb Besario-  
nis dze Jughashvili) 89  
Staniszkiś Jadwiga 92  
Strache Heinz-Christian 38  
Surkov Vladislav 71  
Szymański Sebastian 10, 13
- Śledź Piotr 40  
Ślufińska Monika 67
- Talbot Paul F. 91  
Tandoc Edson Castro, Jr. 21  
Tenove Chris 15  
Tkachuk Taras Yu. (Ткачук Тарас Ю.) 100  
Tomanek Paweł 13  
Torrey Mike 18–19  
Treisman Rachel 84
- Trzebiński Jerzy 54  
Tsymbursky Vadim 91  
Tyszkiewicz Adrian 83  
Tzu Sun 11
- Usmanov Alisher 73
- Volodin Vyacheslav 71
- Walicki Andrzej 92  
Waltz Kenneth N. 87  
Wasiuta Olga 11  
Weitz Richard 60  
Wesslau Fredrik 38  
Włodkowska-Bagan Agata 42  
Wojnowski Michał 54
- Yeltsin Boris 90
- Zawadzki Jarosław 11  
Zelensky (Zelenskiy, Zelensky) Volodymyr  
16, 22, 43, 76–79, 102, 109, 112–113  
Zevelev Igor A. 90  
Zhovtenko Taras (Жовтенко Тарас) 101  
Zolotovskyy Yuli 89  
Zuckerberg Mark 15

Information security is one the key aspects of modern security and its importance has been significantly increasing in contemporary international relations. This publication presents the results of studies on several key aspects related to this issue. The publication contains results of research on considerations related to information security and its implementation, as well as research on social media, analysed through the lens of the object and subject of disinformation activities.



<https://akademicka.pl>

