International Journal of Religion
2024
Volume: 5| Number 2 | pp. 121 – 130
ISSN: 2633-352X (Print) | ISSN: 2633-3538 (Online)
ijor.co.uk

First Submitted: 20 January 2024 /Accepted: 08 February 2024
DOI: https://doi.org/10.61707/0g2yt516

Information Warfare as an Instrument of Geopolitical Influence on Ukraine: Main Aspects and The State's Response

Tetyana Plazova[1], Oleh Kuz[2], Nina Konnova[3], Dmytro Korotkov[4] and Oleksandr Galushchenko[5]

Abstract

The purpose of the article is to study information warfare as an instrument of geopolitical influence on Ukraine, the main aspects of this problem and certain elements of the Ukrainian side's response to the Kremlin regime's information attacks. To achieve this goal, the methods of comparison, analysis, synthesis and content analysis were used. The results indicate that the Russian side in the information warfare uses both traditional tools, such as the media, troll factories, bot factories, and fakes, and new technologies, such as deepfake. This arsenal is constantly evolving and adapting to technological advances. The Kremlin's main goal in the information warfare is to "undermine" Ukraine from within, creating the impression of close ties between Ukraine and Russia as a Eurasian state. Russian activities go beyond Ukraine, influencing public opinion in European countries, the United States and beyond. "Influence operations use social media platforms to spread individual narratives and sow hostility. To counter Russian influence, a program is being implemented to increase media literacy among the Ukrainian public. Ukrainian television companies are responding to the invasion by creating joint telethons that expand communication channels and counter disinformation. Individual tools, such as podcasts, are becoming important in countering disinformation. Ukrainian radio plays a key role in providing information in the occupied regions, and media literacy projects help to verify information and increase information literacy. Initiatives to develop media literacy and counter disinformation in Ukraine are widespread and effective. Results show that the level of resistance to propaganda has increased, and more than 70% of the population can recognize manipulative tactics. Government and civil society initiatives are working together to combat disinformation. Institutions such as the Center for Countering Disinformation and the Center for Strategic Communications are making an important contribution to the resilience of Ukrainian society.

Keywords: *Russo-Ukrainian War, Manipulations, Information Warfare, International Community, Geopolitics*

INTRODUCTION

In the modern world, information warfare has become an effective tool of geopolitical influence, combining elements of psychology, technology, and strategies for influencing society and political processes. Ukraine, which is going through a difficult period of historical and political changes, has become a special target for information attacks by various actors. These threats were particularly intensified by the Kremlin regime, which actively used the modern information space to discredit the Ukrainian government and society. This created a public basis for the start of aggressive actions in Russian society, and some elements were also used against democratic audiences in Europe and America. This case became one of the biggest information conflicts of the twenty-first century. The free use of Russian propaganda spread to the digital space and was aimed at supporting aggressive military actions, denying the crimes of the Russian army, creating a domestic Russian audience, etc. Thus, the active use of information as a weapon is a very relevant object for consideration and research. So are the attempts of the Ukrainian side to counter such Russian information aggression.

Research Problem

[1] Department of Military History, National Army Academy named after Hetman Petro Sahaydachnyi, Lviv, Ukraine, E-mail: tanialviv17@gmail.com
[2] Department of International Relations, Political Science and Practical Philosophy, Faculty of International Relations and Journalism; Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine, E-mail: oleh.kuz@hneu.net
[3] Department of International Relations, Faculty of International Relations and Journalism, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine, E-mail: nina.konnova@hneu.net
[4] Department of International Relations, Political Science and Practical Philosophy, Faculty of International Relations and Journalism, Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine, E-mail: Dmytro.korotkov@hneu.net
[5] Department of Information Protection, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, Ukraine, E-mail: mamr3379@gmail.com

The research problem related to the proposed topic is, first, the need for a thorough study and understanding of the impact of information warfare on modern Ukrainian society and political processes. This problem arises from the numerous challenges that Ukraine faces in the context of information and psychological influence by external and internal actors. It is about understanding how information attacks affect the formation of public opinion, attitudes towards the government and the situation in the country. This may include analyzing the spread of fake news, distorted facts, and politically oriented information. Equally important is the study of how cyberattacks and other cyber threats are used to influence political processes and the country's critical infrastructure. Another controversial issue is to consider the impact of information warfare on international relations, especially on Ukraine's interaction with other countries and international organizations, and to identify and develop strategies to improve information security, identify and counter information threats at various levels, including the state, corporate and public sectors. These aspects interact and create complex issues that require in-depth research to understand information dynamics and determine the best strategies for the state's response to these and other challenges.

Research Focus

One of the key aspects of our research will be to study the methods of information warfare used to influence Ukrainian society. To this end, we will examine the spread of disinformation through various media and social networks, the manipulation of public opinion, and the use of cyber threats to attack critical infrastructure. Uncovering such techniques will allow us to understand their consequences for the stability and security of the country. It will also analyze the responses of the Ukrainian state to these challenges. This includes the adoption and implementation of information security strategies, the establishment of cybersecurity principles, and the development of an appropriate legal environment. Special attention will be paid to the effectiveness of the implemented measures, as well as to the implementation of other possible ways to improve the system of response to information threats. Finally, constructive approaches to strengthening Ukraine's information security and responding to information challenges will be proposed. These include the development of public relations strategies, the expansion of international cooperation, and the introduction of the latest technologies for countering information threats.

Research Aim and Research Questions

The purpose of the article is to analyze information warfare as an instrument of geopolitical influence on Ukraine, the main aspects of this influence and certain elements of the state response. The realization of this goal implies the identification of several tasks, primarily related to the overall impact of information warfare on Ukraine and modern geopolitics, and determining the extent to which this phenomenon affects international relations. To this end, it is also proposed to study the interaction of external actors in the field of information warfare and its impact on regional stability.

BACKGROUND THEORY

Data Mining

To achieve the goal of the study, the method of synthesis was used, which allowed us to process the scientific literature and recorded cases of information aggression and to highlight certain elements that need to be strengthened for the further policy of countering information aggression. Similarly, the use of the method of analysis made it possible to identify certain manifestations of information campaigns directed against Ukraine by Russian special services. This method made it possible to create a picture of individual manifestations of digital campaigns, which can be an important contribution to further study of this issue. The method of content analysis allowed us to select media sources and information platforms, including news sites, social networks, official statements of government agencies, and other sources reflecting public opinion and official positions. This method was used to select relevant scientific literature. The literature was searched and analyzed using databases of scientific journals, from which the most recent and most cited papers were selected using relevant keywords, whose contribution to the coverage of the problem is extremely high. The content analysis method was used to identify the main theoretical concepts covered in the scientific publications. By comparing the results with the existing practices in Ukraine, it was possible to highlight promising ways to continue the fight

against the Kremlin regime's information campaigns. Problematic elements and promising areas for further elaboration of these issues were also identified.

LITERATURE REVIEW

Certain aspects of this problem have been developed in research. Pawełoszek et al (2022) [1] examined the impact of artificial intelligence and digital technologies on the future of the legal sphere, discussed the use of technology in legal processes and possible prospects. Sviderska (2022) [2] examined the use of digital propaganda and information security risks in the context of the Russo-Ukrainian war. Krawczyk and Wiśnicki (2022) [3] analyzed the means and techniques of information warfare in the context of operations conducted by the Russian Federation during the war in Ukraine in 2022. Azieva et al (2021) [4] studied access to television programs using information technology in some countries. Baek (2022) [5] traced the impact of the war in Ukraine on East Asian geopolitics. Maraieva (2022) [6] considered the formation of a new information worldview of the future, trends in the development of the information space and their impact on the perception of the world. Dov Bachmann Putter and Duczynski (2023) [7] highlighted the peculiarities of the use of disinformation companies in the context of the Russo-Ukrainian war. Bryczek-Wróbel and Moszczyński (2022) [8] described the key aspects of the transformation of modern information warfare. The philosophical aspects of the impact of information campaigns in wartime are described in detail by Durmishi and Durmishi (2022) [9]. Shakun (2022) [10] is also important for this work, describing the key principles of the development of the modern information society and the role of mass communication in it. Storey-Nagy (2022) [11] focused on the analysis of disinformation, ideas without borders and the war in Ukraine, and the impact of disinformation on events in the modern world. Štrucl (2022) [12] analyzed cyber operations in the context of Russian aggression against Ukraine. Perhaps, the impact of cyberspace on modern warfare is considered. As we can see, researchers have taken different approaches to analyzing the possibilities of information warfare against Ukraine, rightly considering the Kremlin regime as its main initiator. However, the question of the Ukrainian side's response to information provocations and confrontation in the digital sphere requires further consideration.

RESULTS AND DISCUSSION

Russia's Information Warfare: Features Of Conduct and Tools

Russia's arsenal of information warfare tools is extensive and varies depending on the specific goals. Traditional tools include mass media, troll farms, bot farms, and fake news [13; 14]. In addition, texts, videos, audio recordings, images, memes, etc. serve as channels for disseminating information. It is worth noting that certain political, social, and even religious groups can also act as tools in the field of information warfare (see Figure 1).

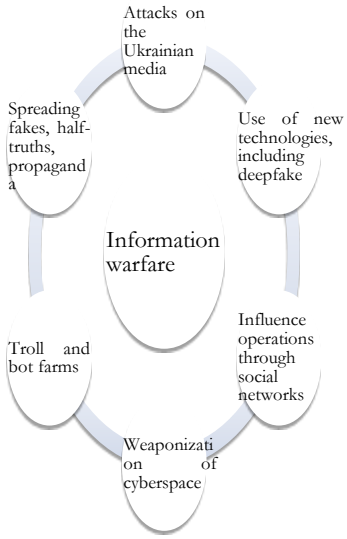

Fig. 1. Key aspects of Russia's information warfare tools

Source: based on [1], [13], [14], [15].

The main goal of the Kremlin is to "undermine" Ukraine from within by promoting the belief that Ukraine and Ukrainians are closely linked to the image of Russia. The media not only disseminates information about military conflicts, but also becomes a target of attacks, especially when it comes to spreading false information. In this complex landscape, media users become victims of an information war waged by both traditional media and online outlets. The multifaceted tools used in Russian information warfare continue to evolve, adapting to technological advances and the changing landscape of global communications. In addition to the traditional tools mentioned above, new methods have emerged, including deepfake technology, which allows for the creation of realistic video or audio recordings with fabricated content. Deepfakes are a serious concern because they can convincingly portray people saying or doing things they have never done, blurring the line between fact and fiction.

In addition, the concept of "influence operations" has gained popularity, where social media platforms are used to spread individual narratives and sow hatred. State-sponsored actors can use social media algorithms to amplify divisive content, target specific demographic groups, and manipulate public opinion. This strategic use of social media amplifies the impact of disinformation campaigns by reaching a wide and diverse audience. The weaponization of cyberspace has also become a key aspect of information warfare. State-sponsored hacker groups can engage in cyber espionage, attempting to infiltrate government networks, media organizations, and critical infrastructure. In addition to collecting sensitive information, these cyber operations can disrupt communication channels and compromise data integrity, exacerbating the chaos caused by disinformation [16].

In the context of Ukraine, information warfare extends beyond its borders, with Russia actively engaged in attempts to influence public opinion in European countries, the United States, and beyond [17], [18]. The use of fake websites, social media accounts, and manipulative content remains a worrying trend, with Russian embassies and cultural centers playing a role in spreading narratives that question the effectiveness of sanctions against Russia and promote divisive ideologies.

Administration S. Kiriyenko, Kremlin "technologists" and media representatives involved in psychological operations (PSYOP), the themes of a new disinformation campaign against Ukraine were approved. The goal is to discredit Ukraine and influence its global partners.

Recognizing that the usual methods of Russian propaganda, such as promoting outright lies, are losing their effectiveness among most Ukrainians, who have developed a certain "immunity" to Kremlin disinformation during the ongoing conflict, a change in strategy is evident. This time, Russian propagandists are trying to capitalize on the real problems Ukrainians face, albeit through their own interpretive lens. Russian propagandists focus on narratives around mass mobilization, widespread corruption in Ukraine, the perceived "failure" of the Ukrainian Armed Forces' counteroffensive, and the alleged lack of trust in Ukraine among Western partners.

Russian propaganda seeks to convey to Ukrainian audiences the idea of an imminent "mass mobilization" that will supposedly affect all citizens, regardless of gender, age, health status, and even minors [19]. The second aspect of this disinformation campaign is to undermine Western support for Ukraine. In the information space, Russian narratives spread stories about secret agreements that talk about peace in exchange for territory. The disinformation package also includes the promotion of a narrative called "Counteroffensive Failed," in which propagandists spread false information about the increasing number of war graves and battlefield failures. The Russians have also initiated attempts to blame these alleged failures on discrediting Ukrainian military leaders and officials [20]. The constant focus of Russian political strategists remains on "corruption in Ukraine," attempting to convince Ukrainians that the authorities are not effectively fighting corruption by alleging budget embezzlement, procurement irregularities, and apparent impunity for corrupt officials. This narrative is presented in stark contrast to the supposedly corruption-free environment in all European partner countries.

The next narrative in the Russian propaganda playbook aims to demonstrate the "easy and beautiful life of Ukrainians in the occupied territories," supported by fabricated evidence of high salaries, low prices, sufficient supply of goods, infrastructure development, and reconstruction of destroyed housing.

It has been proven that in addition to Ukraine, Russia intends to spread provocative and manipulative materials in Germany, France, Israel, and the United States. Russian embassies and cultural centers are actively involved in a large-scale disinformation campaign in Europe, using fake websites and social media accounts to spread narratives about the alleged ineffectiveness of sanctions against Russia, the prevalence of Nazi ideology among Ukrainian officials, and the negative consequences of accepting Ukrainian refugees in Europe. There have been reports of pro-Russian content related to the war in Ukraine being disseminated through fake sites that mimic well-known French publications such as Le Monde, Le Parisien, and government websites.

Modern hybrid information warfare is implemented in various ways. Critical infrastructure objects emerge as particularly vulnerable in this context, facing an elevated susceptibility to sabotage, terrorist acts, and unauthorized interventions. In the prevailing circumstances, Russia strategically employs life support facilities as weapons, utilizing them for moral and psychological terrorism against the civilian population. This calculated approach aims to amplify internal destabilization within the country, emphasizing the necessity for complex, coordinated measures at the national level. Ukraine is urgently tasked with adapting its state policy to effectively counter the numerous tools employed by the aggressor country in this hybrid war. These tools explicitly target the dismantling of Ukraine's sovereignty and integrity. The ongoing full-scale war initiated by Russia poses a substantial threat not only to military and industrial facilities but also to vital elements of critical infrastructure. Moreover, alarming incidents of deliberate destruction targeting critical infrastructure objects are intended to inflict considerable harm on the normal living conditions of the civilian population. Faced with these challenges, the state's management of critical infrastructure protection is assigned multiple objectives. These include the establishment of new institutions and the optimization of existing ones in the defense sector, the development of public institutes and state-public cooperation, and the formulation and implementation of state policies dedicated to ensuring the security of the population and safeguarding critical infrastructure facilities.

How does Ukraine protect itself from Russian propaganda?

As information warfare becomes more sophisticated, the need for media literacy and public insight becomes more critical. Governments, media organizations, and technology platforms must develop robust strategies to counter disinformation and protect the integrity of information channels. Ongoing information warfare efforts underscore the need for international cooperation to address the challenges posed by state-sponsored disinformation campaigns in an interconnected and technologically advanced world.

In the aftermath of the full-scale invasion, the joint response of major Ukrainian television channels, including 1+1, UA: Pershyi, Rada, ICTV, STB, and Ukraine 24, resulted in a joint telethon called United News. This joint effort is aimed at expressing the official position of the state. At the same time, recognizing the need to reach an international audience, a Russian-language marathon was launched to diversify the communication channels used during this critical period. On the very day of the invasion, a new initiative, a podcast titled "Russian Fake, Go to...!" was launched, providing an additional platform to counter disinformation.

Although the podcast has gained a significant online following, it is primarily distributed through Ukrainian radio broadcasts. As the only on-air media available in the occupied regions, such as Kherson, Mariupol, Melitopol, Berdiansk, Donbass, and Crimea, Ukrainian Radio acts as a lifeline, providing a "window to Ukraine" for those living under occupation. In regions where other TV channels and FM radio stations are disrupted by power and communications outages, Ukrainian Radio becomes a vital source of information. This broadcasting platform plays a key role in transmitting vital information about humanitarian corridors, demobilization procedures, presidential addresses, and countering hostile disinformation. The "Russian Fake, Go to...!" podcast has not only received a huge response online, but has also become a trusted resource for individuals across the country. People are actively contacting us to verify information they suspect is false, to suggest topics, and to ask questions. In addition, there are many projects in Ukraine aimed at developing media literacy, digital literacy and information literacy. They are based on both university and government activities.

These collective efforts mark a significant departure from the information vacuum observed in 2014. Ukraine's information warfare landscape now includes numerous media organizations and outlets, which produce content that explains the reality of the situation to a variety of audiences. In addition, a powerful network of disinformation countermeasures organizations, including Detector Media, StopFake, and VoxCheck, are actively analyzing the enemy's actions and creating text, audio, and video content in multiple languages.

Strategic initiatives to counter disinformation have been implemented at the government level. The Center for Countering Disinformation at the National Security and Defense Council and the Center for Strategic Communications and Security Information at the Ministry of Culture and Information Policy are at the forefront of these efforts. These entities are actively involved in the fight against disinformation and make a significant contribution to the resilience of Ukrainian society in the information space. In this context, the Center for Strategic Communications and Information Security is important, as it works in three areas (See Figure 2).

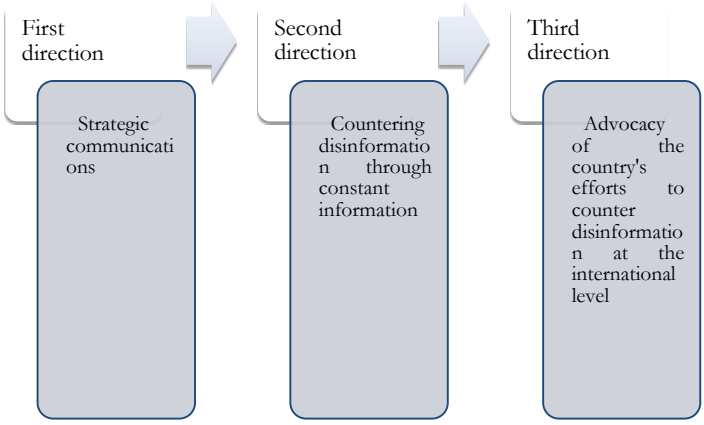

Fig. 2. Main directions of work of the Center for Strategic Communications and Information Security

Source: by the authors

Therefore, the Center's work is aimed at identifying and explaining disinformation in time and promoting the correct and authentic narrative in advance.

The proactive measures taken by organizations like StopFake are supported by research conducted before the invasion, which shows a significant increase in the level of resistance in the country. Today, more than 70% of Ukrainians are not only aware of the existence of propaganda, but also have the knowledge to recognize its manipulative tactics. This is a significant step forward in improving the information literacy of the population and reflects a sustained response to the challenges posed by disinformation in times of crisis [21].

In addition to ongoing initiatives such as telethons and podcasts, recent developments in Ukraine's information warfare landscape include a surge in digital media campaigns and social media activity. Recognizing the global nature of the conflict, Ukrainian activists and influencers are using various online platforms to counter Russian disinformation by sharing real-time updates, eyewitness accounts, and verified information. Hashtags such as #StandWithUkraine and #StopRussianAggression have gained popularity, fostered international solidarity and strengthened the Ukrainian narrative.

In addition, efforts to use new technologies to combat disinformation have intensified. Artificial intelligence and machine learning algorithms are being used to quickly identify and debunk false narratives, allowing for a more flexible response to the dynamic nature of online information warfare. Collaboration with technology companies and cybersecurity experts continues to strengthen Ukraine's digital defenses and improve its ability to detect and neutralize disinformation campaigns in real time [7].

On the international front, diplomatic efforts are complemented by strategic communications initiatives to ensure that Ukraine's perspective is accurately represented in the global media. Ukrainian embassies and cultural centers abroad actively engage with international media, hold press briefings, and use social media platforms to provide real-time updates on the situation, counter false narratives, and build alliances with foreign influencers who support Ukraine's cause.

Additionally, recognizing the importance of disseminating information in multiple languages, efforts were made to expand content creation beyond Ukrainian and Russian. By working with translators and content developers from different linguistic traditions, the goal is to effectively communicate Ukraine's narrative to a wider global audience and counter the potential impact of disinformation in different regions.

In the education sector, there is a growing focus on media literacy programs to equip the public with the skills necessary to critically evaluate information sources. Delivered both in person and through online platforms, these programs empower people to navigate the digital landscape responsibly and separate fact from fiction.

As the confrontation evolves, Ukraine remains at the forefront of information warfare, adapting strategies and leveraging technological advances to effectively combat disinformation [15]. The resilience of its information ecosystem, coupled with international support and collaborative efforts, underscores Ukraine's commitment to protecting the truth in a complex and rapidly changing media landscape.

It is important to note that the Armed Forces of Ukraine, under the command of the Supreme Commander of the Armed Forces, have specialized forces and means aimed at implementing measures to counter negative information influences, including those on military personnel. Historically, various systemic structural units have been engaged in countering such influences (See Figure 3).

In this context, the Main Command Center of the Armed Forces, in particular its structural unit, the Center for Information Monitoring and System Analysis, is responsible for monitoring the information space in order to counteract negative influences on military personnel.

At all command levels of the Armed Forces there are special structural units for moral and psychological support, accompanied by subordinate forces and means, including cultural institutions, psychological support centers and information facilities. These facilities are equipped with technical resources ranging from television and video equipment to mobile audio broadcasting equipment [22].

The Main Joint Center for Information Protection and Cybersecurity is responsible for the technical protection of information and telecommunication systems. This includes ensuring the proper functioning of the Armed Forces websites, which are recognized as an effective tool for disseminating information about the activities of the Armed Forces.

Operational groups of the Armed Forces, such as the Naval Forces Command, include units specializing in electronic warfare (EW). These units take measures to counteract the negative information influence of the enemy by electronic suppression or jamming of harmful transmissions of enemy television and radio stations.

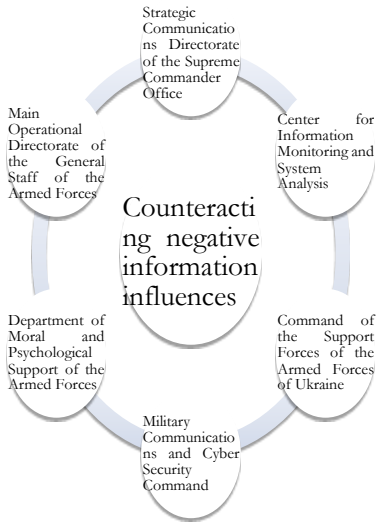

Fig. 3. Countering negative information influences in the Armed Forces of Ukraine. *Source*: by the authors

In summary, the Ministry of Defense of Ukraine, the General Staff of the Armed Forces and the entire structure of the Armed Forces have at their disposal the necessary components of a comprehensive system for countering negative information and psychological influence on military personnel. This multifaceted approach combines strategic communications, information monitoring, cyber defense and electronic warfare to maintain the morale and well-being of the troops. Therefore, as can be seen from the above analysis, the MoD of Ukraine, the General Staff of the Armed Forces and the structure of the Armed Forces have the basic components of a system to counter negative information and psychological influence.

Thus, the findings underscore Ukraine's multifaceted approach to countering disinformation and negative psychological influence, particularly in the context of the ongoing conflict. Ukraine has a joint telethon called "United News" to convey the official position of the state. The launch of the podcast "Russian Fake, Go to ***!" on the first day of the full-scale invasion demonstrates Ukraine's adaptability in using different platforms to counter disinformation. While the podcast has gained significant traction online, its main distribution is through Ukrainian radio, the only broadcast media available in the occupied regions. These efforts are complemented by a surge in digital media campaigns, social media activity, and the use of new technologies [18], [21]. We agree with Rakhimov [23] that artificial intelligence and machine learning contribute to the rapid detection and debunking of false narratives. This increases Ukraine's ability to combat disinformation in real time. Diplomatic efforts, strategic communication initiatives, and cooperation with technology companies emphasize a holistic approach to preserving Ukraine's narrative on the global stage [24]. Within the Armed Forces, structural units of moral and psychological support, as well as specialized troops, play a role in countering negative information influences on servicemen. The Main Command Center, in particular the Center for Information Monitoring and System Analysis, monitors the information space, provides real-time updates and exposes enemy disinformation. The Ministry of National Defense, the General Staff, and the armed forces together form a comprehensive system for countering negative information and psychological influence, including strategic communication, information monitoring, cyber defense, and electronic warfare.

At the same time, the use of individual elements of countering Russian information aggression is quite controversial. In particular, researchers have been drawn to the effectiveness of a single telethon, which looks like a certain anachronism in the context of total digitization of society. According to Lysenko et al [19], the spread of information in the digital space is extremely fast, so it would be important to formulate an adequate response to Russian challenges in the digital environment. The speed of the response is becoming an extremely important feature, and a response in the form of a telethon may lag behind the need. On the other hand, the existence of a single telethon implies the unification of information by the main news agencies. In times of popularity of social networks and messengers, where individuals have a significant impact on public opinion

[6]. According to Prokopenko [25], unification at the level of news agencies often borders on censorship of information that would otherwise be conveyed to society through private digital channels. This technique can harm Ukraine in the international arena, as it positions itself as a democratic country where the right to information can be considered fundamental, even in times of war. Therefore, the existence of such a tool as a single telethon may be unnecessary in the system of countering Russian information challenges.

Thus, we should agree with the researchers that Ukraine's response to disinformation covers a wide range of initiatives in the media, technological, and military spheres [19], [22], [26]. These efforts reflect the country's resilience in preserving its narrative, both domestically and internationally, amid the challenges posed by the ongoing information war [20], [27]. At the same time, promising areas for further development of scientific research are attempts to trace the effectiveness of individual instruments (for example, a single telethon) through the prism of legal justification and impact on society. Since the role of traditional media is limited in times of active integration of digital tools in the presentation of information, it will also be important to study the impact of private influencers (bloggers, columnists, etc.) in the information confrontation.

CONCLUSIONS

Thus, the arsenal of Russian information warfare tools is broad and diverse. Russian information warfare uses traditional tools such as mass media, troll factories, bot factories, and fakes, as well as new technologies such as deepfake. This arsenal is constantly evolving and adapting to technological advances. The Kremlin's main goal in the information war is to "undermine" Ukraine from within. A key strategy is to create the impression that Ukraine is closely tied to Russia as a Eurasian state. This includes not only spreading disinformation, but also using social media and other platforms to shape certain narratives. Media and users become victims of information warfare. Attacks on the media, including the dissemination of false information, are becoming a common phenomenon. Social media and media users are exposed to influences that can distort public opinion and create the impression of false realities. The specific nature of information warfare includes cyber operations. State-sponsored hacker groups are actively engaged in cyber espionage, attempting to infiltrate government networks, media organizations, and critical infrastructure. This not only provides access to confidential information but can also disrupt communication channels and threaten data integrity. At the same time, Russia's information warfare extends beyond Ukraine. Russia is actively influencing public opinion in European countries, the United States, and beyond. The concept of "influence operations" uses social media platforms to spread individual narratives and sow hostility.

Public media literacy is an important aspect of a complex information war. The Ukrainian government, media and technology platforms should develop strategies to counter disinformation and protect information channels. Ukrainian TV companies are responding to the invasion by creating a joint telethon and Russian-language marathon. Aimed at the official state position, these efforts broaden communication channels and counter disinformation. Certain tools (e.g., podcasts) have become important tools for countering disinformation. Ukrainian radio plays a key role in providing information in the occupied regions, and media literacy projects help to verify information and increase information literacy. Initiatives to develop media literacy and counter disinformation in Ukraine are widespread and effective. The level of resistance to propaganda has increased, and more than 70% of the population can recognize manipulative tactics. Government and civil society initiatives are working together to combat disinformation. Institutions such as the Center for Countering Disinformation and the Center for Strategic Communications make an important contribution to the resilience of Ukrainian society. The global nature of the conflict is underscored by activity on social media and online platforms. Hashtags such as #StandWithUkraine and #StopRussianAggression promote international solidarity and reinforce the Ukrainian narrative. For future research, however, it is crucial to determine the need to continue the unified telethon and to characterize the specific methods of working with digital information dissemination channels to counter Russian fakes and propaganda.

REFERENCES

I. Pawełoszek, N. Kumar, and U. Solanki, "Artificial intelligence, digital technologies and the future of law," Futurity Economics&Law, vol. 2, no. 2, pp. 22–32, 2022. https://doi.org/10.57125/FEL.2022.06.25.03

O. Sviderska, "Digital propaganda and risks of information security in the context of the Russian-Ukrainian war," Politicus, vol. 2, pp. 60–65, 2022. https://doi.org/10.24195/2414-9616.2022-2.10

P. Krawczyk and J. Wiśnicki, "Information warfare tools and techniques in the context of information operations conducted by the Russian Federation during the 2022 war in Ukraine," Cybersecurity and Law, vol. 8, no. 2, pp. 278–286, 2022. https://doi.org/10.35467/cal/157216

G. Azieva, S. Kerimkhulle, U. Turusbekova, A. Alimagambetova, and S. Niyazbekova, "Analysis of access to the electricity transmission network using information technologies in some countries," E3S Web of Conferences, vol. 258, p. 11003, 2021. https://doi.org/10.1051/e3sconf/202125811003

S.-w. Baek, "War in Ukraine and Challenge for East Asian Geopolitics," ECONOMY AND SOCIETY, vol. 135, pp. 198–229, 2022. https://doi.org/10.18207/criso.2022..135.198

U. Maraieva, "On the formation of a new information worldview of the future (literature review)," Futurity Philosophy, vol. 1, no. 1, pp. 18–29, 2022. https://doi.org/10.57125/FP.2022.03.30.02

S. Dov Bachmann, D. Putter, and G. Duczynski, "Hybrid warfare and disinformation: A Ukraine war perspective," in Global Policy, 2023. https://doi.org/10.1111/1758-5899.13257

P. Bryczek-Wróbel and M. Moszczyński, "The evolution of the concept of information warfare in the modern information society of the post-truth era," Przegląd Nauk o Obronności, vol. 13, pp. 48–62, 2021. https://doi.org/10.37055/pno/152620

L. Durmishi and A. Durmishi, "A philosophical assessment of social networks impact on adolescents' development in conditions of unlimited access to information," Futurity Philosophy, vol. 1, no. 2, pp. 27–41, 2022. https://doi.org/10.57125/FP.2022.06.30.03

N. Shakun, "Anthropological dilemmas of information society development modern stage in the context of globalisation challenges," Futurity Philosophy, vol. 1, no. 3, pp. 52–63, 2022. https://doi.org/10.57125/FP.2022.09.30.04

J. Storey-Nagy, "Disinformation, Ideas without Borders, and the War in Ukraine," Hungarian Studies Review, vol. 49, no. 2, pp. 220–223, 2022. https://doi.org/10.5325/hungarianstud.49.2.0220

D. Štrucl, "Russian aggression on ukraine: Cyber operations and the influence of cyberspace on modern warfare," Contemporary Military Challenges, vol. 2022, no. 2, pp. 103–123, 2022. https://doi.org/10.33179/bsv.99.svi.11.cmc.24.2.6

O. Batrymenko and D. Nelipa, "Fake news in social networks as a manipulative tool of information warfare," Visnyk of the Lviv University, vol. 45, pp. 86–91, 2022. https://doi.org/10.30970/pps.2022.45.10

M. Wenzel and K. Stasiuk-Krajewska, "Disinformation related to the war in Ukraine," Mediatization Studies, vol. 6, pp. 23–38, 2022. https://doi.org/10.17951/ms.2022.6.23-38

O. Verholias, "Special information operations as a geopolitical change tool," Law Bulletin, vol. 9, pp. 16–22, 2019. https://doi.org/10.32850/2414-4207.2019-9.02

O. Gushchyn, O. Kotliarenko, I. Panchenko, and K. Rezvorovych, "Cyberlaw in Ukraine: current status and future development," Futurity Economics&Law, vol. 2, no. 1, pp. 4–11, 2022. https://doi.org/10.57125/FEL.2022.03.25.01

T. Zawadzki, "Examples of russian information war activity at the beginning of Ukrainian crisis," International Conference KNOWLEDGE-BASED ORGANIZATION, vol. 28, no. 1, pp. 146–150, 2022. https://doi.org/10.2478/kbo-2022-0023

K. Hong, "Paradox of Hybrid Warfare: Lessons from the Ukraine War," The Journal of Strategic Studies, vol. 29, no. 2, pp. 53–73, 2022. https://doi.org/10.46226/jss.2022.07.29.2.53

S. Lysenko, O. Marukhovskyi, A. Krap, S. Illiuschenko, and O. Pochapska, "The Analysis of World Information Warfare and Information Security in the Context of the Russian-Ukrainian War," Studies in Media and Communication, vol. 11, no. 7, p. 150, 2023. https://doi.org/10.11114/smc.v11i7.6414

N. Putnik and B. Milosavljević, "Russian information operations in the Ukrainian armed conflict," Bezbednost, Beograd, vol. 63, no. 1, pp. 62–81, 2021. https://doi.org/10.5937/bezbednost2101062p

A. Rogozińska, "The security of Ukraine in the context of information warfare in cyberspace carried out by the Russian Federation," Rocznik Instytutu Europy Środkowo-Wschodniej, vol. 20, no. 2, pp. 107–122, 2022. https://doi.org/10.36874/riesw.2022.2.6

A. Manoilo, "Informational Diversions in the Conflict in Ukraine," SSRN Electronic Journal, 2023. https://doi.org/10.2139/ssrn.4309902

T. Rakhimov, "Research on moral issues related to the use of artificial intelligence in modern society," Futurity Philosophy, vol. 2, no. 2, pp. 30–43, 2022. https://doi.org/10.57125/FP.2023.06.30.03

B. Lawson, J. Glasman, and I. Mützelburg, "Humanitarian Numbers in the Russian–Ukrainian War," Journal of Humanitarian Affairs, vol. 5, no. 1, pp. 52–61, 2023. https://doi.org/10.7227/jha.102

O. Prokopenko, "Some aspects of the state information policy of the modern state: definitions of the future," Futurity Economics&Law, vol. 2, no. 4, pp. 60–72, 2022. https://doi.org/10.57125/FEL.2022.12.25.08

R. Khardel and V. Vyzdryk, "Cinema as a Tool for Influencing Historical Consciousness in Russian-Ukrainian Information Warfare," Codrul Cosminului, vol. 26, no. 2, pp. 281–302, 2020. https://doi.org/10.4316/cc.2020.02.001

Y. Kuryliuk, S. Khalimon, S. Filippov, "Criminological Profile of Corrupt Border Guard (Ukrainian Experience)," Journal of Legal, Ethical and Regulatory, vol. 24, pp. 1–7, 2021.