Information Warfare in the World and Information Security Issues in the Context of the Russian-Ukrainian War

Bogdana Cherniavska[1,*], Serhii Shevchenko[2], Vasyl Kaletnik[3], Hryhorii Dzhahupov[4] and Tetiana Madryha[5]

[1]PhD in Law, Associate Professor, Department of Theory and History of State and Law, Faculty of Law, National Academy of Management, Kyiv, Ukraine, Guest Researcher at the Vrije Universiteit Amsterdam, The Netherlands.

[2]Interregional Academy of Personnel Management, Kyiv, Ukraine.

[3]Doctoral Student, Department of Constitutional and Administrative Law, Faculty of Law, National Aviation University, Kyiv, Ukraine.

[4]Candidate of Legal Sciences, Professor, Deputy Dean of the Faculty in Teaching and Methodological Work, Kharkiv National University of Internal Affairs, Kharkiv, Ukraine.

[5]PhD of Political Sciense, Associate Professor, Department of Political Institutes and Processes, Faculty of History, Politology and International Relations, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk, Ukraine.

Abstract: The development of information warfare in the world and the issue of information security in the context of the Russian-Ukrainian war play an important role in the context of ensuring international stability and favorable further economic, social, and political development. An essential research direction is to characterize the theoretical, practical, and methodological foundations of information warfare, its features, structural elements, and objectives. The legal nature of information warfare deterrence is an important aspect of the study in this article. The possibility of ensuring legal deterrence of information attacks and preventing the development of information warfare is a prerequisite for overall international stability. In the article, the current legal aspects of responding to information warfare and key regulations ensuring the information security of the international space are analyzed. The peculiarities of information warfare development are studied from the perspective of modern armed conflicts and the key reasons for their occurrence, which are accompanied by the practice of information warfare. Attention is paid to the issues of information warfare in Ukraine from the standpoint of strengthening the need for prompt response to information campaigns, timely detection, and prevention by taking appropriate measures in the economic and political space. The key principles and directions of using information warfare as a tool for gaining competitive advantages are described. The results of the article indicate that the practice of information warfare is spreading to the general political space in the world and that there is an increasing need to regulate the circulation of harmful information while ensuring access to it. This study may be useful for building an effective legal framework and principles of information security based on the experience of information warfare in Ukraine.

Keywords: Information Warfare; Information Security; International Security; Propaganda; Information Campaign; Digital Technologies; Socio-Political Space.

1. INTRODUCTION

The issue of information warfare is important because it affects the formation of the socio-political space and can provide competitive advantages or weaken the enemy in the geopolitical arena. Information warfare is a form of "cold" military conflict or its precondition. Usually, information warfare is a tool for economic, political, and ideological struggle, which is less brutal than a military campaign. However, in today's world, the use of information warfare has become a negative factor that has led to the biggest crisis in European space - the military conflict in Ukraine. The latter was caused by the aggressive actions of the aggressor country and its information warfare against Ukraine, which became a victim of this conflict. The policy of untimely response to the risks of Russia's information campaign, as well as the possibility of spreading its economic influence to the EU energy and commodity markets, led to the military conflict in Ukraine. Therefore, there is a need to improve the quality of legal responsibility and develop the practice of ensuring international information security. Such actions will

*Address correspondence to this author at the PhD in Law, Associate Professor, Department of Theory and History of State and Law, Faculty of Law, National Academy of Management, Kyiv, Ukraine, Guest Researcher at the Vrije Universiteit Amsterdam, E-mail: b.c.h.cherniavska@vu.nl.

help to strengthen the position of the international community and prevent the threat of a new military conflict. The current practice of preventing information warfare is primarily based on special educational activities and the use of the media as the main tool for countering information campaigns. However, in such conditions, there is a need to improve the quality of information circulation, the ability to control it and carefully check its reliability before using it. A separate area of development is to strengthen the role of the UN as the main institution dealing with the policy of countering information campaigns and ensuring the stable development of the information environment in the world. The war in Ukraine has led to the development of crisis processes in the global space and has actualized the need to counteract information attacks by the aggressor country. An essential factor in overcoming the problems of information campaigns and reducing the level of information warfare is the development of a legal mechanism for regulating and creating responsible bodies to control and monitor these processes.

The article aims to analyze information warfare in the world and information security in the context of the Russian-Ukrainian war, as well as key aspects of its impact and consequences on the global geopolitical space. An important research direction in the article is the analysis of current practices of information campaigns and information attacks in the context of military conflicts or covert economic warfare. The article focuses on the information war in Ukraine, which began in 2014 and had negative consequences in the form of a large-scale military conflict. The article also examines the legal aspect of regulation, deterrence, and development of information wars by key international bodies. The legal aspect has the character of a deterrence tool, but the article also explores the peculiarities of practical counteraction to information campaigns, in particular through the media and the development of digital infrastructure.

2. LITERATURE REVIEW

The issue of information warfare, as well as the peculiarities of its factors and development factors, are being studied in the scientific community to counter information campaigns and identify key aspects of their conduct. Bolton (2021) notes that information warfare is a means of gaining a competitive advantage in the international arena. Moreover, such a war aims to spread its ideology and level the forces of the opposing country on economic or geopolitical grounds. Dwoskin (2022) believes that information warfare in the current development environment has important implications for international security. It is also necessary to take into account the international experience of management in national security (Akimov, O., Troschinsky, V., Karpa, M., Ventsel, V., & Akimova, L., 2020), take into account in the adaptive management of enterprise resource planning (Akimova, L., Akimov, O., Maksymenko, T., Hbur, Z., & Orlova, V., 2020). Information warfare also has an indirect effect on energy, namely power plants, which can have a large impact (Popov, O. O., Iatsyshyn, A. V., Iatsyshyn, A. V., Kovach, V. O., Artemchuk, V. O., Gurieiev, V. O., ... Kiv, A. E., 2021). The authors advise not to forget about the provision of legal mechanisms for information security in the conditions of digitalization (Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S., 2022), to improve strategic planning of national security of the state system in the conditions of informatization of society (Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., & Mysyk, A., 2022). Another group of authors draws attention to the financial and economic security of markets in the process of European integration (Novak, A., Pravdyvets, O., Chornyi, O., Sumbaieva, L., Akimova, L., & Akimov, O., 2022), not forgetting innovative approaches in the development of human potential in public administration (Semenets-Orlova, I., Shevchuk, R., Plish, B., Grydiushko, I., & Maistrenko, K., 2022). According to Hudson (2022), the key principle of information attacks are the use of speculative issues that can exacerbate the socio-political situation in a country and contribute to its destructive state. Hurst (2022) argues that the practice of information warfare began to be implemented in the 20th century, where the propaganda of ideologies was used to strengthen one's position and weaken the influence of the opponent. In the context of modern warfare, the use of information warfare is a tool for gaining economic advantages and the possibility of conducting such activities in the long term. According to Pahlke (2022), information warfare is a consequence of the weak legal framework of the international environment, which contains a clear definition of information security but does not have effective tools to respond to or prevent information attacks. The problem with information warfare, according to Snopok (2022), is the complexity of jurisdiction, which creates problems in prosecuting the use of information campaigns. Therefore, this practice is popular in any country in the world. Ringhof (2022) points out that strengthening the role of international law in information security should be a key priority for the further development of the international community and contribute to an effective mechanism for the protection of human rights and freedoms. According to Ryan (2022), the development of the Internet has led to a wave of new technologies for conducting information and psychological attacks aimed at discrediting political forces and lobbying for their interests. The use of information technology, as noted by Valiushko (2015), is a key tool for information warfare. Therefore, the development of digital infrastructure and ensuring its security should become a priority for the leading states. According to Wojnowski (2017), information warfare in the world will be a continuous process, as its existence implies the existence of different ideologies, which is a factor in building a democratic society. In such conditions, the key principle is the use of legitimate tools for ideological and political struggle. Merchant (2022) believes that the further development of information wars may be the strengthening of the role of the use of media resources, and the use of imitation materials to strengthen the role of a particular social community and protect its interests. Thus, in modern scientific research, considerable attention is paid to information wars and their development. However, due to the current geopolitical situation, there is a need to improve international information security, which creates the expediency of this study.

3. MATERIALS AND METHODS

When writing this article, materials from periodicals characterizing the peculiarities of the state and development of information warfare in the world and the key parties involved were used. The article uses scientific research methods, in particular, analysis of practical aspects of the development of information warfare in the world, characteristics of key categories of information attacks, and information campaigns. For example, the search method was used to analyze the theoretical aspects of the essence of information warfare, its main structural elements, and the features of its implementation in the era of digital technologies. The application of the synthesis method made it possible to characterize the practical aspects of information warfare, as well as the possibilities of its further development and counteraction. In addition, the author analyzes the legal aspect of using legal and regulatory frameworks to counter information attacks, the possibilities of ensuring the security of the international information space, and tools for preventing information wars. The method of induction was used to characterize the key aspects of the development and consequences of the information war in Ukraine and the peculiarities of its further development in the current global environment. The article also utilizes materials from periodicals that characterize the peculiarities of the state and development of information warfare in the world and its key participants. The article employs the methodology of researching the theoretical basis for the introduction and conduct of information warfare as a prerequisite for conducting a military campaign and achieving economic competitive advantage in the international arena. The issues of information warfare are studied from the perspective of the current global conflict and the need to strengthen international information security, as well as the use of the legal framework for regulating the activities of the media and combating international information terrorism of the aggressor country. The above research methodology helps to outline the results of the study. They may be useful for analyzing the current practice of countering information warfare and the peculiarities of its conduct in the context of the modern development of digital technologies and infrastructure.

4. RESULTS

The development of information warfare in the world and information security plays a key role, as the use of information influence can become a factor in the development of political opinion and lead to the introduction of certain harmful trends. The key goal of any information warfare is to change political opinion and discredit the ideology and principles of functioning of a certain social environment. As a rule, information wars are waged between the largest states and representatives of various ideologies. The modern policy of information warfare is to use the media to influence society and conduct appropriate rhetoric. As a rule, information warfare is accompanied by imitation facts, speculation on acute issues, and the use of such tools to destabilize the mood in the country to weaken the position of a political force and lobby its interests in the country or the international arena.

In today's world, information wars are spreading rapidly and are used in the context of the strategic policy of countries to achieve political, economic, and other goals of oligarchic elites. In particular, a striking example of information warfare is Russia's use of language-based speculation, which has been going on since 2014. In addition, the aggressor country is pursuing a policy of discrediting the Ukrainian government by using social platforms, media outlets, and tools to ensure that forces favorable to the political authorities are on its side in the Ukrainian space. An information war is also being waged for a long period between China and the United States, which uses harsh rhetoric and discrediting materials at the international level. The key reasons for the information war are economic issues, such as customs duties and the circulation of goods between countries, as well as territorial aspects. In particular, this concerns the status of the Taiwanese peninsula, which is a producer of electronic chips. Information campaigns are conducted by both the United States and China to gain strong international positions. For instance, there was a long information campaign between Israel and Iran, which were involved in a long military conflict. The key aspects of this war were speculation on the historical use of territories, religious aspects, and speculation on the expediency of armed conflict.

Common to any information warfare in the modern world is the use of special tools aimed at discrediting political elites and leveling the value of a political idea. Often, an information campaign and successful rhetoric can contribute to achieving economic benefits and developing socio-economic solutions. An example of this is the Minsk Agreements of 2014, which were initiated by European countries to resolve the conflict between Russia and Ukraine. However, with the use of information attacks by Russia, these agreements became ineffective and aimed at prolonging the military conflict. In 2022, the war led to information attacks on the Ukrainian and European media space, the main aspects of which were the use of means of propaganda of the values of the Eastern space. Furthermore, fictitious facts from the Russian side were widely used in the international arena to cut off financial assistance to Ukraine, as well as to stop the supply of weapons, ammunition, etc. However, such an information campaign was completely lost due to Ukraine's powerful information counteraction, as well as coverage of key international legal acts that emphasize the illegality and barbarism of the aggressor country.

The regulatory and legal nature of information warfare and information security is of key importance, as after the Second World War, the conduct of the Cold War became a popular practice, and specialized information attacks were conducted through the spread of ideologies and the use of some media. Among the key aspects of changes in the regulatory and legal framework is the emergence of the Internet. The peculiarities of the legal environment for the protection of information security are of key importance for the European Union, as the protection of European values and the promotion of their formation is a common vector of political development. To improve the quality of legal regulation on the availability of information, peculiarities of its use, and regulatory aspects of the media, the UN is used to counteract information attacks and specialized campaigns.

Implementation of such a legal policy makes it possible not only to consolidate a high-quality legal international environment for information security but also to create responsibility for information attacks and define them as an illegal policy in the context of the functioning of international law. In particular, the issue of defining the terminology and

Table 1. Characterization of key Legal Provisions of Information Security in the World.

Document	Characteristics
UNGA Resolution A/RES/64/211 of December 21, 2009	Implements a general policy for the development of information security in the international environment.
UNGA Resolution 53/70	Defines the key principles of international information security practice.
UNGA Resolution 54/49	Describing international information security in the military sphere and as a result of hostilities.
UNGA Resolution A/RES/57/53	Establishing a procedure for countering information warfare or any other threat to international information security.
UNGA Resolution 73/266, 2018	Ensuring the integration of states into cooperation in the context of building international information security.
The OSCE Declaration №633	Implementation of an open policy on the use of the Internet, ensuring the constitutional right of citizens to access information.
Directive 2007/65/EC	Measures that should regulate the information space of the European Union and prevent harmful information for the development of the EU.

Source: compiled by the author.

mechanisms of functioning of the information environment of the international space is considered with due regard to the peculiarities of the functioning of a high-quality environment and the possibility of using specialized tools aimed at improving such a policy. The legal framework makes it possible to create tools for the European Union to counteract information campaigns, as well as to have deterrents to the development of information wars. UN resolutions are actually in place in every country in the world and have clear provisions on information warfare and the main means of countering it.

The use of legal and regulatory frameworks is popular in countries such as the United States, China, the United Kingdom, and others. The key principles are the protection of the domestic information environment and the possibility of using the main tools to counter information campaigns, ensuring natural political competition, and the absence of influence of international attacks on the formation of the information environment. Regulation of the legal activities of the media is a key factor in improving the quality of independent opinion and free information space. In today's realities, legal regulation of internationally important publications needs to be improved, including the introduction of restrictions to avoid propaganda of Russian rhetoric. Such a legal policy can serve as a factor in improving the quality of the legal and strategic positions of the European Union countries in the field of information security. The key legal provisions used to counter information wars and are important for ensuring international information security are shown in Table **1**.

Based on the data in Table **1**, it can be argued that the current policy of international space, in particular of organizations such as the UN, uses legal aspects to ensure the information space and strengthen information security. This practice is useful from the perspective of preventing the aggravation of military conflicts in the world during the 21st century and the possibility of timely response to information attacks and other information campaigns aimed at destabilizing the international information environment.

However, this practice of strengthening the quality of countering information attacks has shortcomings in the legal sphere, as the regulation of information and its circulation on the Internet should be improved. In the absence of liability for conducting information attacks on the Internet, the possibility of bringing to real responsibility is a difficult and time-consuming process, which allows speculation on acute issues in the international space. Furthermore, information campaigns are often initiated by other states or special services, which can only be countered by using technical infrastructure and building their own information space. In most cases, the international community does not use prosecution of certain bodies or the leadership of information campaigns, which is a negative trend and a prerequisite for information campaigns and wars.

In 2022, the war in Ukraine led to processes related to the information environment and to the improvement of the quality of information attacks and discrediting of the European Union and other countries to lobby the interests of the aggressor country in the UN and to take a stronger international position. An important factor in information warfare is the support of the parties behind such campaigns, which makes it more difficult to counter information attacks. In particular, the joint rhetoric of China and Russia regarding the fictitious peaceful settlement of the war in Ukraine is a key area for conducting information attacks on the whole world. The issue of food security in Africa, the use of the European energy crisis, and the supply of weapons from the United States are key tools for Russia's information warfare. Countering these information attacks should be regulated by more stringent measures, including sanctions and prosecution of the bodies that perform the functions of information attacks. In such circumstances, information warfare should be conducted based on building international information security.

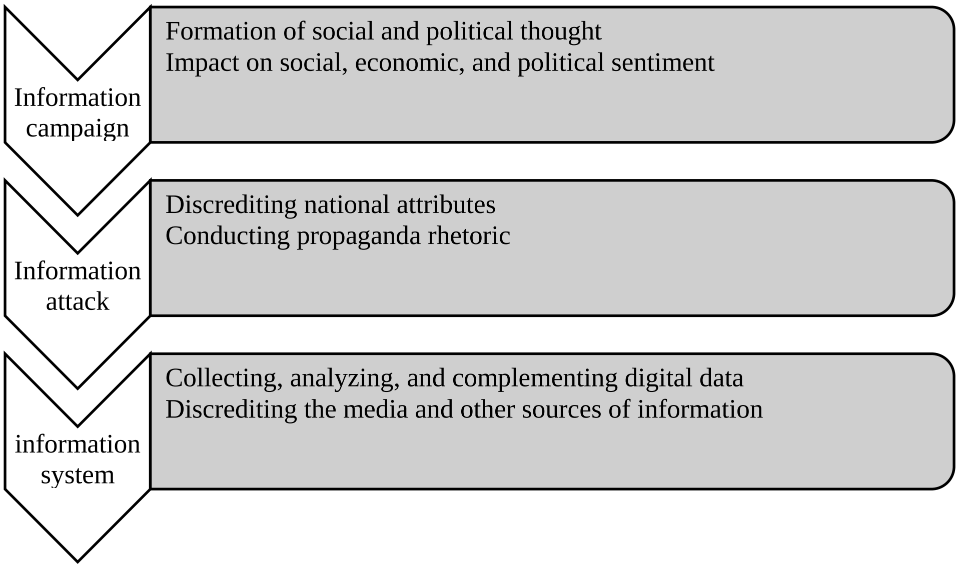
Information campaign
Formation of social and political thought
Impact on social, economic, and political sentiment
Information attack
Discrediting national attributes
Conducting propaganda rhetoric
information system
Collecting, analyzing, and complementing digital data
Discrediting the media and other sources of information

Fig. (1). Key directions of information warfare in the context of the Russian-Ukrainian war.

Source: compiled by the author.

An important direction is the use of digital infrastructure, as it directly affects the ability to use certain tools to ensure the circulation of information and build digital services. Access to information is a key principle of ensuring the rights and freedoms of citizens, as it gives everyone the right to freely use different sources of information and draw their conclusions. This policy is essential for winning the information war. Overcoming the Russian information attack should be aimed at disseminating information about the crimes committed by the Russian authorities and their coverage in the media, as well as using this information to disseminate pictures of the war in Ukraine. The ongoing war has become a key factor in the development of the European Union's military-industrial complex, digital infrastructure, and information security. The issue of improving the quality of information security and countering information attacks is the prerogative of any country's modern policy, as changes in political forces in the world and the restructuring of the global geopolitical space cause several transformational processes in the international legal field regarding the use of information tools of attacks and the possibility of their further development. This includes an increased role of ideology, further construction, resolution of political and territorial issues, a change in orientation to commodity markets, and an escalation of the confrontation between China and the United States. The modern policy of information warfare, as a rule, relies on the use of political technologies and aims to disseminate certain information that would be beneficial to the strategic policy of a particular country. The use of mass media, as well as the creation of media materials, is a factor in improving the quality of any country's information policy. They can help to achieve political goals and contribute to building the information space.

Ukraine's negative experience, as well as being in a state of constant information warfare during 2014-2022, made it possible to identify all the negative consequences of an untimely and inappropriate response to information warfare. On the part of the European Union, timely detection of an information attack and coverage of speculative issues could have helped prevent a military campaign in 2022. However, economic issues and interests counterbalanced such a policy and the possibility of avoiding and preventing war. Therefore, any other policy aimed at building a high-quality international information space should be based on the use of legal norms and the ability to ensure the functioning of digital infrastructure that will counteract information attacks and campaigns. The development of digital technologies provides access to information in virtually any country, so the policy of disseminating information about the real state of political forces in the world and the implementation of policies should become a key factor in the UN's activities. It acts as a regulator of information space security at the global level. In general, the key directions of information warfare in the context of the development of the Russian war are shown in Fig. (**1**).

The directions depicted in Fig. (**1**) are used in practice not only by aggressor countries but also as key means of conducting an information attack. It is also worth emphasizing that information warfare can be not only political but also technical, damaging the financial, logistics, or transportation system. The use of such features in the conduct of information warfare will be of strategic importance and can strengthen positions in the international arena. However, countering information warfare should be much more powerful and have a counter-offensive character. Moreover, the modern information warfare policy should be regulated on a legal basis. Furthermore, international measures and means should be established for countries that counter such campaigns to respond promptly to manifestations of aggression in the information space.

Thus, modern information wars take place in the context of the development and conditions of the Russian-Ukrainian war. The key goal of the development and formation of an information attack is to strengthen Russia's position in the international arena, legalize crimes, and influence the international community to weaken Ukraine and countries that profess democratic values. To counteract such information campaigns, it is necessary to use legal instruments, strengthen the functioning of digital infrastructure, and introduce access to information in countries that have limited access to such information. Educational activities can also be a qualitative factor in overcoming information attacks and winning the information war, which will be of strategic importance.

5. DISCUSSION

The study on information warfare in the world and the issue of information security in the context of the Russian-Ukrainian war shows the development of international law and the strengthening of counteraction to information aggression, which creates qualitative conditions for the development of further security of the global information space. In the context of modern warfare, the focus on high-quality information flow becomes a priority, as information warfare is ongoing and aims to restructure geopolitical forces in the world. The use of an effective policy in information warfare will be of key strategic importance for the international community and will be able to weaken the position of the aggressor country and implement its democratic values. Ukraine's experience shows that an insufficient level of response to the problem of countering information campaigns will have a strategically negative impact that could provoke military conflicts. In such circumstances, there is a need to study the factors and policies of information warfare in 2014-2022, which posed the greatest threat to the modern socio-political space.

The key element used to intensify and conduct information warfare is the media, as well as special platforms, blogs, and other means that allow the dissemination of certain ideas and narratives to society. Legal regulation of such activities is of strategic importance for further policy. The key issue of media regulation is to strike a balance between freedom of expression and the need to ensure legal security and prevent the spread of harmful ideologies. Therefore, building a strategy to counteract information campaigns and the spread of harmful ideologies should be based on a special analysis and preliminary research. Further research on ensuring the legal security of the information environment should be carried out from the point of view of finding effective tools to counteract such policies and serve as a factor in the development of international information security. In particular, an important issue is a possibility of using the media to improve the positioning of different views in the context of the spread and use of information warfare.

One of the priority areas of research should be the use of digital infrastructure and strengthening its protection. Most state secrets are stored in special registers based on the use of digital technologies. Access to these registers is a priority for the aggressor country. Therefore, policies to improve the quality of protection of such technologies and the possibility of their further development will serve as a factor in ensuring collective security in the world and the possibility of protection against the impact of information campaigns. Conducting analytical research on the use of digital technologies to ensure information security will serve as a means of preventing information campaigns aimed at discrediting political forces, ideologies, or the development vector of a particular country. A developed digital infrastructure allows not only stores information and analyzes its use but also provides analytical tools for conducting information and psychological attacks and the possibility of their further development. In general, the prevention of information warfare and practices aimed at neutralizing the results of information campaigns will be most effective in the modern world of digital technologies, so there is a need to develop and ensure their functioning.

6. CONCLUSION

Thus, it can be concluded that information warfare is a set of actions and measures aimed at destabilizing the domestic socio-political situation to achieve its own goals and strengthen its position in the international strategic arena. Most of the goals are driven by socio-economic aspects aimed at improving the quality of the country's functioning in the global community. In addition, information warfare can be used by specific social spheres to strengthen the quality of their influence on the development of ideology, as well as the ability to ensure that they are in line with the key strategies of the state. With the spread of the practice of information campaigns by the aggressor country, the modern policy of countering information warfare is becoming more relevant. The development of the war in Ukraine has led to transformational processes that affect the overall state of international information security. As a rule, any information war aims to discredit the political elite, as well as to use the media as the main tool for spreading such an ideology. The international community's practice of legal regulation of information warfare exists, but it is not sufficiently effective, as evidenced by the outbreak of the war in Ukraine, which has been going on since 2014. The information war waged by Russia against Ukraine has led to economic advantages for Russia, in particular in the raw materials and energy markets of the European Union, which has led to an insufficient response to the threat of military conflict. In this regard, it is necessary to improve the quality of legal regulation of the information space and ensure its security in the context of the current dynamic policy of information campaigns. An important factor in monitoring and controlling information security should be strengthening the role of digital technologies and specialized infrastructure. They are used to improve the quality of the information space and the ability to maintain key levers of influence on the information situation. The war in Ukraine has also led to an escalation of the confrontation between key geopolitical leaders and information attacks on countries engaged in the redistribution of commodity economic markets. The impact of information warfare is aimed at weakening the democratic and value-based policies of the European Union and strengthening Russia's authoritarian aggressive policy. To counteract information warfare, it is necessary to use educational means, promote the development of digital technologies, and strengthen support for Ukraine as a tool of resistance to the aggressor country.

REFERENCES

Akimov, O., Troschinsky, V., Karpa, M., Ventsel, V., & Akimova, L. (2020). International experience of public administration in the area of national security. Journal of Legal, Ethical and Regulatory Issues, 23 (3), 1–7. Retrieved from www.scopus.com.

Akimova, L., Akimov, O., Maksymenko, T., Hbur, Z., & Orlova, V. (2020). Adaptive management of entrepreneurship model as a component of enterprise resource planning. Academy of Entrepreneurship Journal, 26 (3), 1–8. Retrieved from www.scopus.com.

Bolton, D. (2021). Targeting ontological security: Information warfare in the modern age. *Political Psychology,* 42 (1), 127–142.

Bondarenko, S., Bratko, A., Antonov, V., Kolisnichenko, R., Hubanov, O., & Mysyk, A. (2022). Improving the state system of strategic planning of national security in the context of informatization of society. Journal of Information Technology Management, 14, 1–24. doi:10.22059/jitm.2022.88861.

Bondarenko, S., Makeieva, O., Usachenko, O., Veklych, V., Arifkhodzhaieva, T., & Lernyk, S. (2022). The legal mechanisms for information security in the context of digitalization. Journal of Information Technology Management, 14, 25–58. doi:10.22059/jitm.2022.88868.

Carter, E., & Carter, B. (2021). Questioning More: RT, Outward-Facing Propaganda, and the Post-West World Order. *Security Studies,* Vol. 30/1.

Dwoskin, E., Merrill, J., & De Vynck, G. (2022). Social Platforms' Bans Muffle Russian State Media Propaganda. The Washington Post.

Fernandez Gibaja, A., & Hudson, A. (2022). The Ukraine Crisis and the Struggle to Defend Democracy in Europe and Beyond: Rising Stakes in the Struggle for Democracy, *International Institute for Democracy and Electoral Assistance*.

Hurst, D., & Butler, J. (2022). Morrison Government Asks Facebook, Twitter, and Google to Block Russian State Media "Disinformation. The Guardian.

Izadi, E., & Ellison, S. (2022). Russia's independent media, long under siege, teeters under new Putin crackdown.

Long, C., Seitz, A., & Merchant, N. (2022). US, Ukraine Quietly Try to Pierce Putin's Propaganda Bubble. AP Ne.

Novak, A., Pravdyvets, O., Chornyi, O., Sumbaieva, L., Akimova, L., & Akimov, O. (2022). Financial and Economic Security in the Field of Financial Markets at the Stage of European Integration. International Journal of Professional Business Review, 7(5). doi:10.26668/businessreview/2022.v7i5.e835.

Pahlke, J., Senftleben, E., & Bodine, A. (2022). Ukraine's Public Broadcaster Saving Lives: UA: PBC Is More Important than Ever. Deutsche Welle.

Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation.

Popov, O. O., Iatsyshyn, A. V., Iatsyshyn, A. V., Kovach, V. O., Artemchuk, V. O., Gurieiev, V. O., ... Kiv, A. E. (2021). Immersive technology for training and professional development of nuclear power plants personnel. Paper presented at the CEUR Workshop Proceedings, 2898 230–254. Retrieved from www.scopus.com.

Ringhof, J., & José, T. (2022). The Virtual Front Line: How EU Tech Power Can Help Ukraine. European Council on Foreign Relations.

Ryan, J., & Seal, T. (2022). U.K. Asks Meta and TikTok to Block RT and Sputnik After EU Ban. Bloomberg.

Semenets-Orlova, I., Shevchuk, R., Plish, B., Grydiushko, I., & Maistrenko, K. (2022). Innovative approaches to development of human potential in modern public administration. Economic Affairs (New Delhi), 67(4), 915-926. doi:10.46852/0424-2513.4s.2022.25.

Shpyha, P., & Rudnyk, R. (2014). The Main Technologies and Patterns of Information Warfare. [In Ukrainian]. *Problems of international relations*, №. 8, 326–339.

Snopok, O., & Romanyuk, A. (2022). Watching, reading, listening: how media consumption of Ukrainians has changed in the context of a full-scale war. E-Pravda.

Stefanicki, R. (2022). Ktoś podrobił stronę Wyborcza.pl, żeby umieścić artykuł kwestionujący zbrodnię w Buczy. Gazeta Wyborcza.

Taddeo, M. (2012). Information Warfare: A Philosophical Perspective, "Philosophy and Technology" 2012, vol. 25.

Theohary, C. A. (2018). Information warfare: *Issues for congress. Congressional Research Service,* 7-5700.

Tsyganov, V. V., & Kadymov, D. S. (2008), Political and economic information wars. *Information War*, 1, 52–63.

Valiushko, I. (2015). Evolution of Information Warfare: History and Modernity. [In Ukrainian]. *Historical and political studios. Series: Political Sciences,* № 2, 127–134.

Wojnowski, M. (2017). Paradygmat wojny i pokoju. Rola i znaczenie materializmu dialektycznego w rosyjskiej nauce wojskowej w XXI w. "*Przegląd Bezpieczeństwa Wewnętrznego*", nr 17, s. 41–43.

Received: May 25, 2023 Revised: May 30, 2023 Accepted: Aug 03, 2023