UDC 34:316.774 DOI 10.17721/2415-88IX.2024.92.331-343

Vitalii Turenko
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
https://orcid. org/0000–0003-0572–9119
e-mail: vitali_turenko@ukr.net

Nataliia Perepelytsia
Taras Shevchenko National University of Kyiv (Kyiv, Ukraine)
https://orcid.org/0000–0003–2889–3990
e-mail: n.perepelytsia.n@gmail.com

HUMANITARIAN POLICY AND INFORMATION SECURITY AS MAIN ASPECTS COUNTERACTIONS SPREADING WAR RUSSIA AGAINST UKRAINE

Abstract

The article explores the specific and foundational aspects of humanitarian policy as a crucial element in countering the information warfare conducted by the Russian Federation against Ukraine. Several key considerations in this effort include:1. promotion of humanitarian values: *a*dvocating and supporting humanitarian values such as tolerance, equality, and respect for human rights play a proactive role for the state; 2. development of educational and cultural initiatives: implementing programs that foster understanding and mutual appreciation among diverse cultures and nationalities is essential. 3. safeguarding citizens' rights and freedoms: authorities should take responsibility for protecting fundamental rights and freedoms, including freedom of speech, the right to information, and privacy; 4. enhancement of media literacy: initiatives aimed at improving media literacy among the population are crucial. individuals with heightened media literacy are less susceptible to manipulation. 5. international collaboration and diplomacy: collaborative efforts and diplomatic endeavors are necessary for exchanging best practices in humanitarian policy and countering information aggression.6. provision of humanitarian assistance: offering humanitarian aid and support to those affected by information aggression is vital.

The importance of safeguarding both state and personal information cannot be overstated, particularly in light of the increasing prevalence of electronic

systems for governance and information exchange, especially amidst the full-scale war Russia is waging against Ukraine. There is an urgent need to bolster measures that ensure the confidentiality and integrity of data to prevent the compromise of sensitive information and maintain trust and efficiency in administrative processes. Furthermore, economic security is a critical concern, as Ukraine's economic well-being relies on defending against cyber threats. Successful cyber attacks can result in data breaches, financial losses, and a decrease in investor confidence, posing a significant risk to economic growth and stability. Therefore, robust information security measures are indispensable for sustaining Ukraine's economic prosperity.

Keywords: humanitarian policy, information security, Russia's full-scale war against Ukraine, international cooperation, information warfare, post-truth, cyber security, fakes, educational and cultural practices.

Introduction

For Ukraine, research on information security holds profound significance due to several compelling factors. Firstly, amid Russia's full-scale conflict against Ukraine, our nation navigates a complex geopolitical environment. This conflict extends beyond conventional military actions to include cyber warfare and dissemination of disinformation, with the latter serving as a potent instrument wielded by Russia. Consequently, understanding and countering these threats are imperative for safeguarding our sovereignty and national interests.

The significance of the research topic lies also in the escalating importance of information aggression as a foreign policy tool in today's world. The Russian Federation actively utilizes informational tactics to shape global perceptions, highlighting the need to explore strategies for combating this aggression. Hence, humanitarian policy emerges as a potentially effective means of resisting informational attacks. Understanding how humanitarian principles can be leveraged to counter and respond to information warfare is crucial in the present context.

Moreover, given the potential impact of Russian government's information aggression on various countries and regions, studying humanitarian policy as an international tool becomes especially vital for devising cooperative strategies and fostering effective interaction. Therefore, thorough exploration and analysis of the research topic can facilitate the development of robust strategies and mechanisms to mitigate information threats and promote international stability.

Therefore, the aim of this article is to conduct a comprehensive examination and analysis of the role of humanitarian policy and information security as effective factors in countering aggression by the Russian Federation. The article seeks to identify the potential of humanitarian policy and information security in reducing the impact of information aggression and enhancing the resilience of society and the international community against manipulations and influence.

The set goal involves addressing the following objectives:

- elaborate on key terms such as "humanitarian policy" and "information warfare (aggression)" to enhance understanding of their interconnection.

- prove the importance of safeguarding both state and personal information, particularly as electronic systems for governance and information exchange become increasingly prevalent.

- analyze how humanitarian policy can serve as an effective tool in countering information aggression, particularly in relations with the Russian Federation.

Methodology

Various methodologies are employed in political science studies of information security, contingent upon the specific objectives and subjects under examination. Below are some of the most prevalent methodologies: case studies—this approach involves delving into particular cases or events pertaining to information security to dissect the underlying causes, repercussions, and remedial actions taken in response to these occurrences; document analysis—this method entails scrutinizing a diverse array of documents, including legislation, policy programs, strategies, and reports, to discern approaches to information security and responses to prevailing threats; modeling and simulation—utilizing this method allows for the examination of potential outcomes under varied scenarios for information security by creating models and simulating diverse situations; benchmarking—this methodology entails juxtaposing different countries or regions to evaluate their respective approaches to information security, legislation, strategies, and outcomes;

By integrating these methodologies, researchers can garner a more comprehensive understanding of information security issues and devise more efficacious solutions. The foundation of our research rested on a framework rooted in comparative and dialectical analysis.

Results of the research

Role of Ukrainian Humanitarian Policy against Russian`s Information War

When discussing the definition of "humanitarian policy," it's crucial to acknowledge its varied interpretations, contingent upon context and research focus. Nonetheless, a common thread is its aim to achieve humanitarian objectives, including the protection of human rights, ensuring social justice, and advancing education and culture to enhance quality of life. In Western literature, humanitarian policy is often defined as:

1) protection of human rights and freedoms: this involves measures to guarantee and safeguard fundamental human rights and freedoms.

2) social justice: efforts are made to ensure equal opportunities, combat discrimination, and address social issues to foster greater justice within society.

3) humanitarian values: there's a focus on promoting and disseminating humanitarian values such as tolerance, diversity appreciation, and mutual understanding.

4) development of education and culture: policies are directed at improving education and cultural development to facilitate comprehensive societal progress.

5) humanitarian aid and crisis response: providing assistance during natural disasters, conflicts, or other crises, as well as developing strategies for prevention, is integral.

6) global cooperation: collaboration among nations and international organizations is essential to tackle global challenges like poverty and climate change.

It's important to recognize that the concept of humanitarian policy can evolve and adapt to contemporary challenges and the needs of Ukrainian society. As domestic scholars rightly assert, activities in the sociocultural sphere, policies related to interfaith, interethnic, and linguistic relations, and public diplomacy efforts collectively contribute to social stability, cohesion, and societal reintegration. Ensuring citizens' rights across various humanitarian policy domains is fundamental to fostering a democratic process based on inclusivity and promoting overall societal development. [1, p. 128].

"Information Aggression" refers to a type of military tactic utilized to sway public opinion, influence democratic processes, and foster negative perceptions about other countries or organizations. This strategy entails employing informational tools such as mass media, social networks, and internet resources to disseminate disinformation, manipulation, and fake news with the goal of achieving political or military objectives.

Ukrainian researcher I.V. Patlashinska aptly observes that Russian propaganda primarily aims to discredit the Ukrainian government, armed forces, and society as a whole. This includes spreading false information about alleged "neo-Nazis" in Ukraine, with the intention of diminishing Ukraine's significance and influence on the global stage. Furthermore, Russian propaganda highlights supposed issues with specific "Nazis" and "Banderites," who purportedly oppress the Russian-speaking population in Ukraine.

However, since 2014, Ukraine has made substantial progress in preparing for information warfare. Clear communication channels with society have been established, panic dissemination has been thwarted, and cooperation with Western partners has been strengthened, ensuring they receive accurate information about military developments. Consequently, Ukraine has effectively portrayed an accurate depiction of the military situation, dispelling doubts regarding the identity of the enemy and their capabilities [2, p. 87].

The functioning of information aggression encompasses several key aspects, including:

1) disinformation: this involves intentionally spreading false or misleading information to deceive and manipulate public opinion.

2) narrative building: crafting and disseminating specific narratives that serve the aggressor's interests, often aimed at discrediting the target country.

3) hybrid warfare tactics: integrating conventional military tactics with informational and psychological warfare methods to achieve strategic objectives.

4) social media manipulation: exploiting social media platforms to propagate propaganda, sow discord, and amplify divisive narratives.

5) cyber attacks: utilizing cyber means to compromise information systems, disrupt communication, and conduct espionage.

6) psychological operations (psyops): Employing psychological tactics to influence and manipulate the perceptions and behaviors of the target population.

Understanding these aspects is crucial for developing effective countermeasures against information aggression.

It's important to identify and analyze various forms of information aggression as they significantly impact society, political processes, and international relations. The Russian full-scale war in Ukraine underscores the importance of filtering information, conducting quality fact-checking, and resisting destructive informational attacks from the enemy. The course of this war is influenced not only by achievements on the front lines but also by social media users, media professionals, civic analysts, and investigators. Therefore, it's crucial to approach all content responsibly—both the content we consume and the content we share.

Research on information aggression in a political context can be conducted using various approaches and methodologies. Here are some key approaches:

- investigation of information sources: identifying sources that spread information aggression, analyzing their structure and nature, and assessing the reliability and authority of the information they disseminate;

- media analysis: studying the reaction and interaction of the media with information aggression, identifying media and information trends, and analyzing the choice of narratives, words, and images used in informational materials;

- analysis of social media: monitoring and analyzing the impact of information aggression on social media, studying user interaction, and identifying key themes and trends;

- content analysis: analyzing texts, images, videos, etc., to identify explicit or hidden messages and determine key words, themes, and styles used in informational materials;

- audience analysis: studying the characteristics and behavior of the audience interacting with information aggression, identifying target groups and their peculiarities;

- political context: understanding the political background and circumstances influencing information aggression, exploring the goals and strategies of political actors involved in informational campaigns;

- international context: analyzing the impact of international factors on the information aggression of the Russian federation, determining foreign policy goals pursued through informational campaigns.

These approaches contribute to a comprehensive understanding of information aggression and its impact on political processes. Adapting and applying these methodologies effectively address the challenges posed by information warfare in contemporary society. These principles can be employed individually or combined for a comprehensive analysis of Russia's information aggression in the political context.

As emphasized by D. Dutsyk, the full-scale war has underscored the need for increased media literacy among officials at various levels, the development of effective methodologies for engaging new vulnerable audiences (such as residents of regions occupied after February 24, 2022), and systematic, well-executed research on media consumption patterns among citizens and their information perception. Such research should form the basis for the development of programs and projects on media literacy [3, p. 246-247].

Consequently, the central focus in combating such potent and diverse forms of information aggression should be humanitarian policy, particularly concerning the defense of civil rights, cultural and educational spheres, and societal understanding. Here are some aspects that, in our view, should be considered:

1) advancing humanitarian values: the state should serve as a vehicle for disseminating and supporting humanitarian values, such as tolerance, equality, and respect for human rights. promoting these values can serve as a counterbalance to information aggression aimed at undermining these principles.

2) development of educational and cultural programs: initiatives should be implemented to foster understanding and mutual appreciation between different cultures and nationalities. this can decrease society's susceptibility to disinformation and stereotypes propagated through information aggression.

3) protection of citizens' rights and freedoms: authorities should ensure the safeguarding of fundamental rights and freedoms, including freedom of speech, the right to information, and privacy. protecting these rights can help prevent manipulation and disinformation.

4) advancement of media literacy: programs and initiatives should be introduced to enhance media literacy among the population. individuals with high levels of media literacy are less vulnerable to manipulation and can critically evaluate information.

5) international cooperation and diplomacy: collaboration and diplomatic efforts are crucial for sharing best practices in humanitarian policy and protection against information aggression. diplomatic measures can contribute to discussions and the development of international standards and norms in this regard.

6) providing humanitarian assistance and support: measures should be taken to aid those who become victims of information aggression. this may include psychological support, community assistance, and other interventions to mitigate the impact of traumatic information.

Therefore, humanitarian policy can serve as an effective tool in the fight against information aggression by emphasizing societal development, human rights protection, and cultural and educational integration.

As an example, several countries are developing strategies to reduce vulnerability to information aggression and have achieved some success in this regard. These examples demonstrate that countries can effectively respond to information aggression by implementing measures to protect their societies and developing humanitarian approaches to information security. Here are a few examples:

A. Baltic countries: Estonia is taking measures for cybersecurity and cyber defense, considering informational aspects. The country is developing strategies to protect against cyber-attacks and implementing programs to enhance media literacy. Lithuania is also increasing its resilience to information aggression, with a focus on cybersecurity and educational projects.

B. Scandinavian countries: Finland is actively enhancing media literacy among its population and investing resources in educating citizens to distinguish misinformation and recognize manipulations on the Internet. Collaboration with various segments of the public and the promotion of critical thinking are also key. Sweden focuses on increasing its society's resilience to information aggression by promoting media literacy and educational initiatives [See: 4, p.178].

Importance of information security as counteaction factor spreading Russian`s war against Ukraine

The conditions surrounding Russia's full-scale war against Ukraine present significant challenges and threats to information security. Key aspects of ensuring information security in such circumstances include cyber security, information warfare, protection of critical information, monitoring and response to threats, international cooperation, education, and training.

Effectively addressing the issue of cyber security requires a comprehensive approach and coordinated efforts at national, regional, and international levels. This involves preventing, preparing for, responding to, and recovering from incidents involving governmental authorities, the private sector, and civil society. Given the current socio-political and informational challenges, determining political, scientific, technical, organizational, and educational strategies and establishing an efficient cyber protection system as part of comprehensive measures against cyber threats will foster the development of an effective mechanism for countering threats in the cyber domain. This includes a proactive response to dynamic changes in cyberspace and the development and deployment of effective means and tools for potential responses to aggression in cyberspace. Such measures can serve as a deterrent against military conflicts and threats in the cyber realm [5, p.150].

Therefore, it is imperative to safeguard critical infrastructure against cyber attacks, including government communication systems, electronic management

systems, and other vital information resources, from hacker attacks and cyber espionage. It is crucial to acknowledge that Russia employs a wide array of information tactics to manipulate public opinion not only within Ukraine but also beyond its borders. Consequently, Ukraine must devise effective strategies to combat disinformation and propaganda, with a particular focus on continuous monitoring and response to threats. Information security systems must undergo constant enhancement to support ongoing monitoring of threats, vulnerability detection, and swift responses to security incidents.

Regarding Ukraine's international cooperation in information security, it is essential to recognize that the effectiveness of combating these phenomena hinges not solely on measures taken at the national level but also on coordinated efforts at regional and international levels. Analysis of regional international organizations' activities in information security, considering the state and nature of information threats, underscores the importance of policy coordination and multilateral cooperation among states worldwide.

An international and national legal examination of information security in Ukraine underscores the significance of freedom of expression, which provides society with a potent tool for acquiring and comprehending diverse ideas and perspectives. Modern and effective information activities can significantly bolster the state's efforts in peacefully resolving crisis situations. Conversely, neglecting or manipulating information may incite radical attitudes, hostility, and potentially catastrophic consequences.

Considering international legal and national measures aimed at ensuring information security, such as the Convention on Cybercrime, the Recommendations of the Committee of Ministers of the Council of Europe on the protection of freedom of expression and information in times of crisis, and the Decree of the President of Ukraine «On the decision of the National Security and Defense Council of Ukraine of October 15, 2021, on the Information Security Strategy,» it is crucial to acknowledge the significant divergence in legal approaches among different countries regarding national legislation on information security. Thus, achieving substantial changes in international legal regulation of information exchange and communications necessitates accounting for these differences. It is equally vital to establish connectivity between domestic and global information infrastructures to prevent conflicts and to align legal regulations across various levels.

Ukraine must continue bolstering its international cooperation with organizations such as the OSCE, NATO, the UN, and the EU across all domains. Whenever feasible, Ukraine should assert its positions and interests in international negotiations and before international courts. Furthermore, there is a pressing need to actively adopt European and international cybersecurity standards, enhance the operations of specialized bodies capable of effective collaboration with relevant EU and NATO entities, and engage Ukraine in joint exercises and training sessions, including with foreign experts [7, p.275].

The integration of information technology into the military domain has opened up new avenues to bolster a nation's defense capabilities against aggressors. In this context, the possession and protection of information resources have gained significance on par with conventional assets such as weapons, ammunition, and transportation. Ukraine's proficiency in the realm of information warfare vis-à-vis Russia will be crucial in realizing the nation's strategic objectives and ultimately securing victory.

Moreover, alongside international collaboration, it is imperative to prioritize comprehensive education and training in cybersecurity and information security to cultivate a cadre of skilled professionals capable of safeguarding the country's interests. To this end, ongoing initiatives should include:

- specialized training programs for information security specialists, covering the detection and neutralization of information and technical threats targeting the nation's information infrastructure and other critical assets;
- tailored training courses for personnel in the information security and information warfare units within the armed forces and relevant ministries and agencies;
- specialized training sessions, including retraining and advanced education, focusing on information security matters for governmental bodies involved in state, military, and corporate governance;
- general education initiatives aimed at equipping the populace with the necessary skills to navigate the complexities of life in an information-driven society [See: 3].

By prioritizing ongoing education and training efforts, Ukraine can strengthen its resilience against emerging threats and effectively mitigate risks to its national security.

Conclusions

Thus, by analyzing and elucidating the functioning of humanitarian policy as a factor in countering the information aggression of the Russian Federation in the conditions of its full-scale war against Ukraine, the following conclusions can be drawn.

Information aggression against Ukraine is a multifaceted, polyvector phenomenon encompassing the creation and dissemination of disinformation, the use of social networks, organized attacks on opponents, hybrid information warfare, manipulation of historical narratives, and influence on elections and political processes. As a counteraction factor, humanitarian policy should also be multifaceted, particularly directed towards promoting humanitarian values, developing educational and cultural initiatives, protecting the rights and freedoms of citizens, enhancing media literacy, fostering international collaboration and diplomacy, and providing humanitarian assistance.

The protection of both state and personal information is of paramount importance. With the proliferation of electronic systems for governance and information

exchange, there is an urgent need to strengthen measures ensuring the confidentiality and integrity of data. Failure to do so not only compromises sensitive information but also undermines the trust and efficiency of our administrative processes. Economic security is another pivotal concern—Ukraine's economic prosperity relies on safeguarding against cyber threats. Successful cyber attacks can lead to data breaches, financial losses, and a loss of investor confidence. Therefore, robust information security measures are essential for sustaining economic growth and stability.

Furthermore, safeguarding the information security of our citizens is imperative. Protecting personal information is crucial, as malicious actors may exploit such data for criminal purposes, including fraud and cyber blackmail. By prioritizing the protection of citizens' information, we can enhance their trust in digital platforms and mitigate the risk of cyber-related crimes. Lastly, international cooperation plays a crucial role in addressing these multifaceted challenges. Ukraine stands to benefit from collaborating with international partners to exchange expertise and intelligence on cybersecurity and combatting cyber threats. By fostering partnerships on the global stage, we can augment our capabilities and enhance our resilience against evolving cyber threats.

References

1. Humanitarian policy in Ukraine: challenges and prospects. (2020). Sinaiko, O. O. (head of author's group), Tyshchenko, Yu. A., Kaplan, Yu. B., Mykhailova, O. Yu., Valevskyi, O. L. & other (2020). Kyiv: NISD. [in Ukrainian].
2. Patlashynska, I. V. (2022). Modern Russian-Ukrainian information war: tasks, methods and features of use. Regional Studies, No. 28, 84-87. [in Ukrainian].
3. Dutsyk, D. (2023). The formation of social stability and critical media literacy - before and during the war. У Glapiak, A. (Red.), Ukraińskie media w obliczu wojny : regulacje prawne i przyskie = Ukrainian media in the conditions of war: legal norms and experience (p. 241-248). Warszawa: Wydawnictwo Akademii Sztuki Wojennej.
4. Clack, T. & Johnson, R. (2021). The World Information War: Western Resilience, Campaigning, and Cognitive Effects. Routledge.
5. Trofimenko, O. G. (2022). Cybersecurity of Ukraine: analysis of the current state. Information Protection, 21(3), 150-157.
6. Chitak, V. & Usmanov, Y. I. (2023). International and national legal analysis of the state of information security of Ukraine in the conditions of armed conflict. Scientific Bulletin of Uzhhorod National University, Series PRAVO, 76(2), 271-277.

Список посилань

1. Гуманітарна політика в Україні: виклики та перспективи. Аналіт. доп. [Сінайко О. О.(кер. авт. кол.), Тищенко Ю. А., Каплан Ю. Б., Михайлова О. Ю., Валевський О. Л. та ін.]. Київ: НІСД, 2020. 126 с.

2. Patlashynska, I. V. Modern Russian-Ukrainian information war: tasks, methods and features of use. Regional Studies. 2022. No. 28. C. 84-87.
3. Дуцик Д. Формування соціальної стійкості та критичної медіаграмотності—до та під час війни. Українські медіа в умовах війни: правові норми та досвід. 2023. С. 241-248.
4. Clack T., Johnson R. The World Information War: Western Resilience, Campaigning, and Cognitive Effects. Routledge. 2021. Pp. 271-277.
5. Трофименко О. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2022. Випуск 21. № 3. С. 150-157.
6. Чітак, В., Усманов Ю. Міжнародний і національно-правовий аналіз стану інформаційної безпеки України в умовах збройного конфлікту. Науковий вісник Ужгородського національного університету. Серія: Право. 2023. Том 2. № 76. С. 271-277.

УДК 34:316.774 DOI 10.17721/2415-88IX.2024.92.331-343

Туренко Віталій Едуардович

Київський національний університет імені Тараса Шевченка (м. Київ, Україна)

https://orcid. org/0000–0003-0572–9119

e-mail: vitali_turenko@ukr.net

Перепелиця Наталія Олегівна

Київський національний університет імені Тараса Шевченка (м. Київ, Україна)

https://orcid.org/0000–0003–2889–3990,

e-mail: n.perepelytsia.n@gmail.com

ГУМАНІТАРНА ПОЛІТИКА ТА ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОСНОВНІ АСПЕКТИ ПРОТИДІЇ ПОШИРЕННЮ ВІЙНИ РОСІЇ ПРОТИ УКРАЇНИ

Резюме

У статті досліджуються засадничі аспекти гуманітарної політики як одного з ключових елементів протидії інформаційній війні, що ведеться Російською Федерацією проти України. Кілька ключових міркувань у цій сфері: 1. просування гуманітарних цінностей: просування та підтримка гуманітарних цінностей, таких як толерантність, рівність та повага до прав людини, відіграє проактивну роль для держави; 2. розвиток освітніх та культурних ініціатив: реалізація програм, які сприяють взаєморозумінню та взаємоповазі між різними культурами та національностями, має важливе значення. 3. забезпечення прав і свобод громадян: влада має взяти на себе відповідальність за захист фундаментальних прав і свобод, зокрема свободи слова, права на інформацію та приватність; 4. підвищення медіаграмотності: ініціативи, спрямовані на підвищення медіаграмотності населення, мають вирішальне значення. люди з підвищеною медіаграмотністю менш схильні до маніпуляцій. 5. міжнародна співпраця та дипломатія: спільні зусилля та дипломатичні зусилля необхідні для обміну кращими практиками в гуманітарній політиці та протидії інформаційній агресії.6. надання гуманітарної допомоги: надання гуманітарної допомоги та підтримки тим, хто постраждав від інформаційної агресії, є життєво важливим.

Важливість захисту як державної, так і особистої інформації неможливо переоцінити, особливо у світлі все більшого поширення електронних систем управління та обміну інформацією, особливо в умовах повномасштабної війни, яку Росія веде проти України. Доведена нагальна потреба в посиленні заходів, які забезпечують конфіденційність і цілісність даних, щоб запобігти компрометації чутливої інформації та зберегти довіру й ефективність адміністративних процесів. Крім того, економічна безпека є критично важливим питанням, оскільки економічний добробут України залежить від захисту від кіберзагроз. Успішні кібератаки можуть призвести до витоку даних, фінансових втрат і зниження довіри інвесторів, що становить значний ризик для економічного зростання та стабільності. Тому надійні заходи інформаційної безпеки є необхідними для підтримки економічного процвітання та національної безпеки України.

Ключові слова: гуманітарна політика, інформаційна безпека, повномасштабна війна Росії проти України, міжнародна співпраця, інформаційна війна, постправда, кібербезпека, фейки, освітні та культурні практики.

Стаття надійшла до редакції 12.03.24