Library Science. Record Studies. Informology.

Library Science. Record Studies. Informology. 20(3), 2024, 21-31
Journal homepage: https://bdi.com.ua/en/journals/journal
Received 29.04.2024 Revised 30.07.2024 Accepted 28.08.2024

UDC 327:314(477) DOI: 10.63009/lsrsi/3.2024.21

Ukraine's cyberdiplomacy in countering Russian information aggression

Iryna Verkhovtseva*

Doctor of History, Associate Professor
State University of Information and Communication Technologies
03110, 7 Solomyanska Str., Kyiv, Ukraine
https://orcid.org/0000-0002-5682-993X

Abstract. Ukraine's counteraction to Russia's information aggression in the international arena after its intervention in 2014 in Donetsk, Luhansk, and Crimea to discredit everything Ukrainian requires the search for effective tools, considering the intensification of processes in cyberspace and the globalisation of communications. The purpose of this study was to prove that one of the effective tools for Ukraine's counteraction to Russian information aggression of an anti-Ukrainian nature in international communications is cyberdiplomacy in its public diplomatic format. The research methodology included a set of general scientific methods (logic, induction, deduction, analysis, synthesis) and specialised methods, such as structural-functional, typological, narrative, and generalisation methods. Since the 1980s, the revolution of information and communication technologies and the cyberneticisation of the global information field have been shaping a new reality – cyberspace. As a communication medium in public diplomatic practices, it substantially affects the communication of governments with the public of foreign countries to influence foreign governments by promoting national ideas, values, institutions, culture, and policies in the information field of the target audience, which affects the image of the state through its perception by the foreign public. In this context, the aggressive policy of the Russian Federation, based on the achievements of the information age, demonstrated how authoritarian countries manipulate people's minds and form beliefs that are favourable to them. Specifically, anti-Ukrainian information activities and the spread of false narratives around the world create a negative image of Ukraine to undermine its international authority and slow down Western assistance to it. Ukraine should actively counter these hostile narratives within the international cyberspace, with cyberdiplomacy in its public diplomatic format being an effective tool, and public/people's diplomacy involving scientists, politicians, students, and the public as one of the instruments, as well as the creation of multichannel media platforms that will host relevant information and educational content with open access to foreign recipients in their languages. In terms of practical value, the findings of this study will serve to develop optimised models of Ukrainian cyberdiplomacy

Keywords: Russian information warfare; diplomacy; public diplomacy; communications in cyberspace; public/people's diplomacy

Introduction

Since the beginning of the Russian Federation's intervention in Eastern Ukraine in 2014, the aggressor country has launched an information war to influence the minds of the public in other countries in addition to Ukrainians towards results desired by the interventionist. Disinformation, information manipulation, fakes, aggressive anti-Ukrainian propaganda narratives aimed at discrediting everything Ukrainian – the government, the state, and the socio-cultural field in general – were manifested. According to V. Ilnytskyj *et al*. (2022), this was the ideological basis for Russia's full-scale military invasion of Ukraine and the substantiation of the expediency from the Russian perspective of changing the Ukrainian political authorities by force according to the wilful decision of the Kremlin political leadership. After 24 February 2022, when Russia

Suggested Citation:
Verkhovtseva, I. (2024). Ukraine's cyberdiplomacy in countering Russian information aggression. *Library Science. Record Studies. Informology,* 20(3), 21-31. doi: 10.63009/lsrsi/3.2024.21.

*Corresponding author

launched an all-out war against Ukraine, this information invasion intensified enormously.

The international diplomatic perspective of Ukraine's counteraction to Russian information aggression in 2014-2024 is reflected in a fragmentary manner by researchers, although attention to this topic in terms of public diplomacy, specifically in terms of the use of cyberdiplomacy in countering hostile information influences, is growing. O. Romtsiv & A. Kharchenko (2023) analysed information confrontation in the context of interstate communication and formulated the task of strengthening international cooperation in the field of information security and open coverage of facts and truthful information about Ukraine. Other Ukrainian researchers have also emphasised the need to transform the image of Ukraine in the international arena, which was shaped by Russian propaganda after 1991. O. Sviderska (2022) pointed out that this threatens to lose the reputational capital of the Ukrainian state. V. Yemets (2023) believed that an effective practice of countering Russian information invasion should be an intensive dialogue with foreign audiences using the tools of public diplomacy.

S. Kovalskyi (2023) investigated counteracting Russian disinformation and propaganda in the Ukrainian information space on the example of the electronic resource "Centre for Countering Disinformation at the NSDC (National Security and Defence Council of Ukraine) of Ukraine" and highlighted the informational, analytical, and educational areas of its work. Although no attention is paid to cyberdiplomacy directly, the analysed experience of refuting propaganda theses, investigation of the mechanism of propaganda influence and methods of information influence in general shows a positive example of the development of such activities, which can underlie the development of cyberdiplomacy structures.

The authors I. Sukhorolska & I. Klymchuk (2022) pointed out that as Russia seeks to destroy trust in Ukraine, diplomatic work with the public in Asia, Latin America, and Africa is urgently needed. It is necessary to disseminate information about the commitment of Ukrainians to universal human values, their heroic struggle against Russian imperialism, for national liberation and their identity.

V. Tsivaty (2023) addressed the technological revolution focused on global initiatives, cyberspace, and artificial intelligence and institutionalised on digital platforms of a new system of international security in real and virtual formats. The researcher stressed that these innovations influence the transformation of the modern model of a diplomat and Ukraine's diplomacy in the dimensions of diplomatic etiquette and intercultural communication, and contribute to a new format of modern diplomacy, its publicity and restraint. According to this researcher, cyberspace is used to establish direct links with the public, which is involved in the development and implementation of information confrontation policy, while cyberdiplomacy is used to constantly improve and adapt diplomacy to the rapidly changing cyber environment.

Researchers V. Pasichna (2023) and V. Dzerkal (2023) focused on certain aspects of the use of cyberdiplomacy tools in Ukraine's international communications in the context of replacing the conventional format of foreign policy and international relations with a digital format. According to these researchers, there are considerable prospects for the use of cyberdiplomacy methods. V. Pasichna (2023) called it an art, a science, and a set of means by which nations protect their interests and promote political, economic, or cultural relations in cyberspace. V. Dzerkal (2023) emphasised that modern cyberdiplomacy is an area of public diplomacy, promoting interaction between countries in terms of contacts between their publics, with the main influence being in the sphere of mass consciousness and political elites. This leads to a dialogue between the official authorities and the public abroad and promotes intercultural communication.

Detailed attention to Ukrainian cyberdiplomacy was paid by V. Matviienko & G. Petushkova (2024), who, for the first time in Ukrainian academic thought, examined the state and prospects of Ukrainian cyberdiplomacy, considering the relevant experience of friendly European countries, specifically Estonia. However, the use of cyberdiplomacy tools in the current Russian-Ukrainian information confrontation was covered by the authors in passing, noting that the concept of cyberdiplomacy is only at the initial stage of development in the world in general and in Ukraine specifically. According to the researchers, the Ukrainian state, like most other countries that practice cyberdiplomacy, needs to reconsider its approaches to it to intensify its use in foreign policy.

Overall, researchers have hardly analysed the state and prospects of Ukraine's cyberdiplomacy in countering Russian information aggression in the context of public diplomacy as a component of international communications.

The purpose of this study was to prove that one of the effective tools for countering Russian information aggression of an anti-Ukrainian nature in international communications is Ukraine's cyberdiplomacy in its public diplomatic format.

Scientific novelty. For the first time, Ukraine's cyberdiplomacy in the format of public diplomacy is described as an effective tool for countering Russian information aggression with an emphasis on the use of public diplomacy methods.

The methodology of the study included a set of general scientific methods (logic, induction, deduction, analysis, synthesis) and a series of special methods: structural and functional analysis, typology, narrative, generalisation. The method of structural-functional

analysis helped to consider cyberdiplomacy as an area of public diplomacy, to determine the specifics and prospects of using cyberdiplomacy tools in this context to counter Russian information invasion. The method of typology helped to identify the means of counteracting hostile information activities and to define public/people's diplomacy as a promising area of cyberdiplomacy in its public diplomatic format. The narrative and generalisation methods were used in the context of understanding the specifics of Ukraine's cyberdiplomacy tools in countering Russian information aggression in the context of cyberspace globalisation and the evolution of public diplomacy in the context of the digitalisation of the international communication space.

Communications in cyberspace and public diplomacy

According to the Oxford English Dictionary (2024), the term "public diplomacy" was first used by the London newspaper "The Times" in 1856 to refer to overt activities and specific official efforts to influence foreign public opinion to achieve diplomatic goals. The modern interpretation of this concept, which refers to a type of diplomatic activity, was initiated 60 years ago by American researchers J. Nye and E. Gullion, who defined public diplomacy as an instrument of soft power in international communications. Public diplomacy complements classical diplomacy with new methods, engaging the societies of communicating countries in diplomatic dialogue. This intensifies intercultural communication, shapes the positive image of states, and contributes to the preventive and peaceful resolution of conflicts and wars (Verkhovtseva, 2023). In the early 2020s, M.V. Trofymenko (2023) proposed to understand public diplomacy as an integral category that, while functioning in synergy with the government and in coordination with other dimensions of foreign policy and international processes, also contains signs of autonomy and self-organisation.

In the last third of the 20th and early 21st centuries, the nature of public diplomacy changed. The main reason for this is primarily the growing influence of the public and the strengthening of interpersonal contacts. Therewith, an important characteristic of public diplomacy has become the way in which it communicates between the government and the public of other countries to promote understanding of national goals and policies, values, culture to influence foreign governments through their citizens (Kukalets, 2020).

However, qualitative shifts in public diplomacy are also driven by the new realities of global social communications, which have been influenced by the scientific and technological revolution and the emergence of innovative communication technologies that have formed a fundamentally new space of human existence – cyberspace. It is extraterritorial and virtually devoid of geographical restrictions. According to D. Dubov (2014), in the global dimension, cyberspace was an information space and at the same time a communication environment. It is created by a set of information processes based on information, telecommunication, information and telecommunication systems and their management, which are united by common principles and rules. L. Piddubna (2016) emphasised that cyberspace is one of the leading factors of the socio-cultural environment and at the same time a factor that affects all spheres of public life – economic, social, political, spiritual and contributes to the formation of the global information space and the functioning of the "network society" (M. Castells). Human life in cyberspace takes place in parallel in the environment of social reality and in its copy – the virtual world generated by technical and technological means. Because of this, a person simultaneously acts as a consumer, receiver, recipient of social information, and at the same time its autonomous subject, which leads to fundamental changes in people's minds and generates qualitatively new types of communication. As a result, there is a redistribution of values in the choice of opportunities for self-realisation of different social groups. Considering this, cyberspace is actively interfering with the structures of power, promoting the formation of e-governments and the virtualisation of political life, which is subject to a "network" logic.

In July 2000, the signing by the presidents of the eight leading industrialised countries of the world (G-8) of the Charter of the Global Information Society (Okinawa Charter) acknowledged the transition to a new stage of society development due to the impact of information and communication technologies on social processes. At the same time, it is recognised that global informatisation has become the basis for a fundamentally unfamiliar environment of confrontation between adversarial states – cyberspace. This new cyber dimension of international relations poses great challenges to the policy of deterrence, as the quality of information and its availability, along with the use of modern information technologies, causes substantial changes in the policies of states, which affects the nature and system of public administration overall. States involved in global information processes should pay special attention to cybersecurity issues. This problem is of paramount importance because of its connection with the security aspects of politics, economy, e-services, energy, transport, and other key areas of society. Therewith, there are no principles for the existence and use of cyberspace. Specifically, the use of information technology for military purposes is not regulated by international law. This turns cyberspace into one of the most powerful challenges to sustainable development and requires close attention of governments and the world community to threats to global development of a political and socio-cultural nature. Therewith, the subjects and objects of cyberspace are a person, society, and the state (Lukianchikova, 2013).

According to V. Matviienko & G. Petushkova (2024), the main problems in cyberspace related to the human factor are largely geopolitical in nature. The challenges of cyberspace are more related to the success of negotiations and political discussions on its governance. The main problem with cybersecurity is not so much preventing attacks as it is the political will of individuals and organisations to take responsibility for regulating aspects of cybersecurity. Furthermore, it is important to understand how these actors can limit and hold states or international actors accountable for malicious activities in the cyber domain. International law cannot fully regulate cyberspace due to the rapid development of technology, which requires constant adjustments. Although the UN has proposed 11 norms of responsible state behaviour, they are non-binding, and many countries have their own policies that contradict these norms. This creates controversy at both the international and national levels.

Researchers A.V. Tarasiuk (2019) and I.V. Alekseenko (2022) emphasised that, considering that globalisation processes erase the boundaries of national identity, the cyberneticisation of the information space is a fundamentally new phenomenon where information is formed, transformed, transmitted, used, and stored, which affects individual and social consciousness, information infrastructure, and information itself. According to the apt remarks of I. Pronoza (2020), due to the ability to disseminate information in large volumes across continents and international regions almost instantly, modern media influence the world political agenda and communication processes on a global scale. This creates the preconditions for the creation, development, and dissemination of information weapons. It should be added that it can target the identity of societies within individual countries, regions, and even the global one.

A. Marushchak (2022) pointed out that the approaches of different countries to social media regulation are at an early stage and change according to national interests. However, while democracies guarantee citizens freedom of speech and access to information in their constitutions, ensuring free and fair participation in political processes and public life in general, in authoritarian countries, through media technologies and the use of epistemic means of manipulating public opinion, the opposite is happening – the achievements of the information age with its digitalisation of communication processes are used to manipulate people's consciousness to promote the necessary ideas and form beliefs favourable to political authorities. First of all, this applies to the Russian Federation.

By hybridising soft power and propaganda, Russian soft power has become an extension of Russian propaganda and a means of implementing aggressive expansionist policies. Therewith, the aggressor country turns the values of Western liberalism outwards, attacking it with its own means (Komar, 2022). Overall, the Russian political authorities' approach to information confrontation is part of a global strategy involving cyber strikes and information operations against democratic actors in international relations. The goals of this strategy are Russian dominance in the post-Soviet space as an imperial sphere of influence, along with the expansion of Russia's political, economic, and military hegemony around the world, to strengthen its status as a great power and form a polycentric model of the world. One of the tools on this path is to reduce the influence of Western democratic values, institutions, and systems (Sunhurova, 2022).

O. Danilyan & O. Dzoban (2022) pointed out that the tasks of information weapons used by Russia are directly related to the mobilisation of supporters and the expansion of target audiences in the international arena. Therewith, considerable efforts are being made to create a virtual illusory "picture of the world" as a parallel reality characterised by transformed values, beliefs, and behaviour. These efforts are aimed at influencing the mass consciousness not only inside Russia, but also outside – at the population of other countries, including Ukraine. Under such conditions, the impact of digitalisation on diplomatic activity, especially in its public diplomatic format, together with conventional methods of foreign policy and the use of online technologies and social media, is turning public diplomacy into a tool for modelling public opinion no less effective than social media, mass media, and mass communication media in general. However, according to I. Holovko (2022), most of the classical instruments of public diplomacy and soft power require long preparation and are not easy to change in the short term. For example, organising a diaspora abroad, exporting a dominant cuisine/food culture to the world, influencing local music to the global public, establishing international television channels and especially news agencies, influencing social media through host countries, exporting high-quality films and TV series, and creating glocalised (globalised + localised) radio and television channels in the target country require defined plans, support projects, and considerable time resources overall. Considering this, as the leadership of the Ministry of Foreign Affairs of Ukraine points out, new areas of international cooperation are opening, involving cultural tools and information technologies in the format of media, social networks. This will facilitate communication and cooperation between states (At Lviv University..., 2023).

Therefore, the task of Russia's information weapons is to mobilise supporters and expand the audience in the international arena by replacing real beliefs. In this context, digitalisation and public diplomacy are becoming powerful tools for shaping public opinion on a par with conventional media and social media.

Cyberdiplomacy as a tool for international communications

Considering the globalisation and digitalisation of the information space and cyber threats to international communications, cyberdiplomacy has become a response to the information challenges of modern time. It is based on the concept of soft power and is an effective tool for reducing uncertainty, eliminating risks and preventing potential conflicts in cyberspace. According to A. Barrinha & T. Renard (2017), cyberdiplomacy was a relatively new concept, although the term has been used before, but mainly to describe e-diplomacy activities. Overall, cyberdiplomacy is defined as diplomacy in cyberspace, or as the use of diplomatic resources and the performance of diplomatic functions to secure national interests in cyberspace. The principal issues on the cyberdiplomacy agenda include cybersecurity, cybercrime, confidence building, Internet freedom, and Internet governance. This allows positioning cyberdiplomacy as an institution of international society, specifically when cyberdiplomacy interacts with actors of the global society. The term is also used to describe the evolution of public diplomacy in the digital age. The goal of cyberdiplomacy is to gradually change behaviour and attitudes towards the space of peaceful coexistence, defined by clear rules and principles: from a system of interactive units to a society of states. In this respect, cyberdiplomacy is a fundamental basis of international society for cyberspace.

In Ukraine, cyberdiplomacy means the use of diplomatic means and initiatives to protect state interests in cyberspace. Diplomats may be tasked with establishing cooperation and dialogue between state and non-state actors at various levels, preventing cyber races, and developing global norms for cyberspace. The principal elements of cyberdiplomacy are strengthening cyber capabilities, building trust and respecting and improving norms in the cyber domain (Matviienko & Petushkova, 2024).

The starting point of cyberdiplomacy is considered to be the publication in 2011 of the US International Strategy for Cyberspace, which became the world's first government document to focus entirely on the international aspects of cyberspace and relies on three pillars to achieve its goals: diplomacy, defence, and development. The strategy served as a roadmap to enable U.S. government departments and agencies to better define and coordinate their roles in international cyberspace policy, and a call to the private sector, civil society, and end users to strengthen efforts through partnership, awareness, and action to achieve the future people all want. The strategy set out the principal objectives (Fig. 1). To implement the Strategy, the Office of the Coordinator for Cyber Issues was created, which is fully dedicated to cyber issues in the foreign policy dimension.

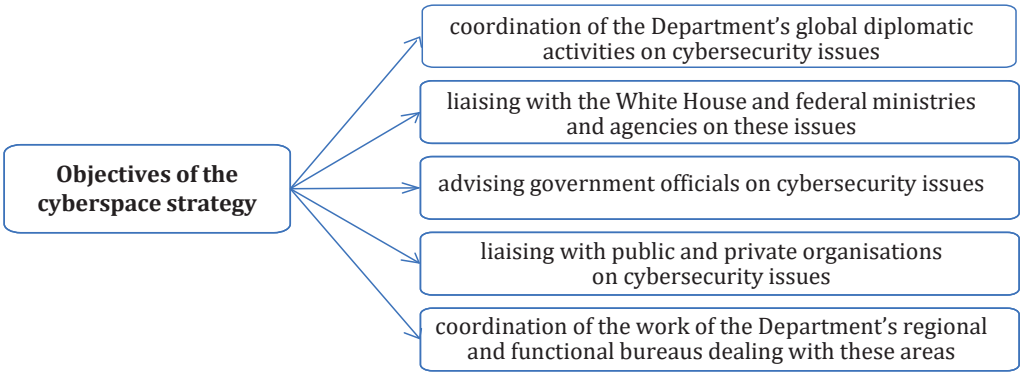

Figure 1. Objectives of the cyberspace strategy

Source: compiled by the author based on V. Pasichna (2023)

V. Dzerkal (2023), in the context of analysing the tools of cyberdiplomacy in the implementation of the state's foreign policy, emphasised that, relying on information and communication technologies (ICT) to achieve diplomatic goals, cyberdiplomacy uses new media, social networks, blogs, and other analogous media platforms in the global network, which are used to promote their interests by state structures, primarily foreign policy bodies, and relevant non-governmental structures.

The web of cyberdiplomacy is expanding and deepening at a rapid pace, gradually creating a cyber international society. The global community is facing increasing difficulties in attributing cyberattacks, and there are concerns about the possible escalation of conflicts between participants due to the unpredictable consequences of cybercrime. International efforts are aimed at expanding cyberspace governance from national and regional initiatives to a unified global approach (Barrinha & Renard, 2017). In different countries, the respective diplomatic services use Internet platforms to communicate directly with the target audience of another country, disseminate important information among its citizens, conduct social surveys. Therewith, it is important for cyberdiplomacy to develop communication strategies by monitoring and analysing information, as well as tracking reactions to cyberdiplomatic activity. In this context, the

effective use of social media and e-diplomacy tools overall contributes to the effectiveness of international communication, raising the authority of the state, improving the image of political leaders, attracting supporters, and exerting influence on opponents. However, no less important, according to H. Al-Muftah *et al*. (2018), was the fact that social networks are becoming potential bases for resolving international conflicts.

In 2013, the European Union (EU) External Cyber Coordination Directorate noted in the context of EU cyberspace coordination that "there are very few countries where national cyber coordination is effective, and the state can speak with one voice in all international fora". Less than a decade ago, diplomats were called upon to regulate cyberspace, which until then had stayed outside the sphere of diplomacy. The situation is changing, and the number of cyber diplomats involved in bilateral and multilateral contacts at all levels around the world is growing. In 2015, the EU recognised the critical importance of further developing and implementing the EU's comprehensive approach to cyberdiplomacy at the global level and stressed the conformity of this area with the EU's fundamental values, such as democracy, human rights, the rule of law, including the right to access information, privacy, freedom of expression, ensuring that the Internet is not used to incite hatred and violence and stays, with strict respect for fundamental freedoms, a forum for free expression in full respect of the law. One of the goals of the EU's activities in this area is to enable citizens to access information that will allow them to fully enjoy the social, cultural, and economic benefits of cyberspace, specifically by promoting the creation of more secure digital infrastructures (Draft Council Conclusions..., 2015).

In the 2010s and early 2020s, the North Atlantic Alliance significantly intensified its public diplomacy communication activities. It uses online media, social media platforms to engage in discussions of security issues (Yakovenko & Piskorska, 2018). In this context, substantial attention is paid to technologies, information weapons, propaganda operations in the wars of the 21st century, and the significance of strengthening cyberdefence and resilience at all levels is acknowledged. In 2016, NATO recognised cyberspace as an operational domain, alongside land and sea, which launched a drive to strengthen the Alliance's cyberdefences. In June 2021, a new comprehensive cyberdefence policy followed, recognising that cyberspace is always subject to competition. In this regard, NATO has convened the first-ever North Atlantic Cyber Coordinators Council. Therewith, cyberdiplomacy in the NATO armed forces, especially in the United States, has substantially changed the attitude of key players towards the geopolitical and civilisational confrontation. This was emphasised in May 2022 at the first International Conference on Cyberdiplomacy "Building global digitalisation: Building trust and security through cyberdiplomacy", organised by the National Institute for Research and Development of Informatics in Bucharest in partnership with the Romanian Ministry of Foreign Affairs (Demianenko, 2018; NATO Deputy Secretary General..., 2024). The event brought together ambassadors, academics, and experts from the international cyber and defence community to promote cutting-edge research and innovation. In his opening speech, NATO Deputy Secretary General Mircea Geoană pointed to the growing daily dependence on digital assets and vulnerability to cyber attacks and incidents.

Ukraine's cyberdiplomacy in countering information aggression

Apart from the important potential of cyberdiplomacy considering the current conditions of development of information and communication technologies in the global dimension, the role that this diplomatic tool can play in organising counteraction to information aggression against a particular country is equally important. This is critical in the context of Ukraine's confrontation with Russian information aggression, which has targeted everything Ukrainian since 2014 – the government, state, society, culture, and identity of Ukrainians. In spreading the ideas of Slavic unity and the "Russian world" around the world, the aggressor country uses systems of organisational, propaganda, psychological. and informational influence, relying on the resources of the media space. The focus of Russian aggressive influence has been on the political leadership of Ukraine and the command of its Armed Forces to create distrust in them. Furthermore, the ideas of racism and inter-ethnic intolerance are being spread in Ukraine. Russia is also trying to convince the international community of systematic violations of the ceasefire by the Ukrainian authorities (Dzhus, 2022). However, the key purpose of Russian information sabotage is to undermine Ukraine's international authority, create a negative image of Ukraine and prevent large-scale military, economic and financial assistance from European countries, the United States and other allies, as well as aggressively influence the consciousness and subconscious of the addressees (target audience) – the public of the world (Zelenko, 2024). Overall, Ukrainian researchers have identified the main Russian narratives about Ukraine, which include a series of theses (Fig. 2). A. Savchuk (2015) pointed out that the Kremlin is trying to tarnish the image of Ukraine in the West and generally make the information field in which Ukraine appears dirty. The study also emphasises that the Kremlin's information war is a war against the whole of Europe, not just Ukraine. To implement such information and communication tasks, the Russian leadership uses considerable financial resources to support pro-Kremlin media. Specifically, in 2021 alone, the pro-government Russian media were allocated about USD 1 billion (One billion dollars for the war of meaning..., 2023).

Figure 2. Russian narratives of hostility towards Ukraine
Source: developed by the author based on N. Vashchenko (2020)

In terms of Ukraine's information policy in the international format, an urgent task is to develop mechanisms to counter disinformation by the aggressor country, which should be based on the fundamental constitutional principles of freedom of speech in the context of the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other fundamental international legal documents (Marushchak, 2022). According to R.A. Mikhailovsky & I.M. Budur (2023), it is much easier to defend their positions in the information confrontation for those countries that have a harmoniously developed and protected information society. However, Ukrainian society has not been prepared to adequately counteract information aggression, and therefore, it is imperative that Ukraine ensure its information security.

Considering such opinions of scientists, as well as trends in the cybernetisation of the global information space, it is logical for Ukraine to use cyberdiplomacy tools in its public diplomatic format to counter Russian information aggression. To the conditions of political, legal, and organisational nature, it is worth first of all add the provisions of Article 17 of the Constitution of Ukraine (1996) on the protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security, which are the key functions of the state and the concern of the entire Ukrainian people. As well as the existence of the term "cyberspace" in Ukrainian legislation. It is understood as an environment (virtual space) that provides opportunities for communication and/or implementation of social relations, formed as a result of the functioning of compatible (connected) communication systems and electronic communications using the Internet and/or other global data networks (Law of Ukraine..., 2024). Furthermore, the necessary legal framework is created by Decree of the President of Ukraine No. 685/2021 (2021), Decree of the President of Ukraine No. 447/2021 (2021) and the Public Diplomacy Strategy of the Ministry of Foreign Affairs of Ukraine for 2021-2025 (2021), adopted in 2021. On this basis, to respond to the challenges of the digital age in a prompt and high-quality manner, in 2023 the Ministry of Foreign Affairs of Ukraine began developing the Strategy of Cyberdiplomacy of Ukraine. A cyberdiplomacy unit has been set up within the Ministry, with active development of the network infrastructure, training, and a system of measures to digitalise the processes associated with the daily activities of the diplomatic service (Deputy Minister..., 2024). By cyberdiplomacy, the leaders of this ministry understand international cooperation in matters related to cyberspace, including the safe and responsible use of new digital tools and technologies, such as artificial intelligence, robotics, quantum computing, state policy on the development of the Internet.

An essential next step was the development of draft amendments to the Law of Ukraine "On the Diplomatic Service", which would entrust this service with the authority to promote and protect national interests in cyberspace – cyberdiplomacy. The legislators propose that cyberdiplomacy should be considered a set of actions and strategies aimed at promoting and protecting national interests and implementing Ukraine's foreign policy goals in cyberspace in the field of international relations, as well as the rights and interests of Ukrainian citizens and legal entities abroad, considering current needs (Ukraine is offered cyberdiplomacy..., 2024).

Equally important in the context of the organisational and legal framework for the development of Ukraine's cyberdiplomacy is the support provided by its allies. Specifically, since 2017, within the framework of the bilateral cyber dialogue between the United States and Ukraine, American allies have committed to provide a framework for further joint efforts to counter disinformation and to make efforts to improve Ukraine's ability to counter Russian disinformation and propaganda in cyberspace, using social media and the media in general (Marushchak, 2022).

However, despite all this, in the early 2020s, there was no intensive discussion of the use of cyberdiplomacy tools in countering Russian information aggression in the academic field and media space of Ukraine. However, as pointed out by A. Barrinha & T. Renard (2017), the victim of aggression, to neutralise the effects of information warfare and repel the aggressor's information attacks, must rely on the same technologies and methods of information warfare as the aggressor,

but to its own ends. First of all, this involves actions in the media space and the use of social media resources. However, even a superficial analysis of the prospects for implementing such tasks can show that the resources of Ukraine's state structures will never be sufficient to repel the information attacks of the aggressor country in the information space in the segment of international communications. And the reason is not the lack of human resources from among the employees of state institutions. The principal reason why it is impossible to use the traditional tools of public diplomacy institutionalised in Ukraine by the MFA to counter Russian information aggression through cyberdiplomacy is the scale of the tasks, as they involve the development of Ukraine's communication with the world community in the context of individual countries, debunking fakes, historical myths, and disinformation messages imposed on the world community by Russia regarding Ukraine.

Considering this, it is advisable to address the resources of public diplomacy as a type of public diplomacy and a tool of cyberdiplomacy. Whereas public diplomacy is carried out by the state, under its leadership or at state expense as part of its foreign policy, citizen/civil diplomacy is implemented by various individuals, legal entities and civil society institutions independently of the state, in the interests of the state, society, or humanity as a whole. The subjects of citizen/civil diplomacy are usually the general public: scientists, students, athletes, business representatives. The goal of citizen/civil diplomacy is to facilitate ongoing contacts between civil society institutions in different countries, a better understanding of the culture and traditions of peoples, mutually beneficial cooperation, the development of international networks, and the creation of an atmosphere of trust and equality. Unlike official diplomacy, citizen/civil diplomacy is carried out on a voluntary, public basis. Specifically, in the United States, according to this concept, every citizen is entitled and even obliged to help the state in its foreign policy activities, and at the same time lobbies for public interests through citizen/civil diplomacy. Citizen/civil diplomacy is implemented through informal contacts of ordinary people, public or non-profit organisations (Bortniak *et al*., 2022).

According to I. Sukhorolska (2022), at the current stage of evolution of citizen/civil diplomacy, it was often called "new public diplomacy", and its main characteristics are as follows: openness and democracy; horizontal relations between participants based on trust and reputation; focus on common interests and values; existence in an environment of healthy competition between state and non-state actors; multilateral communication in a complex network of relations that allows identifying and considering the position of each. It is an interaction in a network of many distinct levels of actors, with civil society groups in different countries acting as initiators, participants, and partners of their states and at the same time target audiences for programmes of foreign governments, organisations, corporations.

Thus, citizen/civil diplomacy can be considered a full-fledged tool of cyberdiplomacy in the context of Ukraine's countering Russia's information aggression. Ukrainian researchers, politicians, journalists, students, and the Ukrainian public in general will promote Ukrainian interests in the world and thus influence the positive image of the Ukrainian state by preparing and publishing content on media platforms and social networks that debunks fake, disinformation, and propaganda narratives of an anti-Ukrainian nature. The language barrier can be a problem in the communication dimension, as it is advisable to speak to the public of another country in its language. One of the effective measures in this regard may be the organisation of multichannel media platforms (websites), where information materials of relevant content, educational content will be posted by reputable scientists, politicians, intellectuals, and will be available to foreign recipients in their languages. Overall, the field for creative activity of the Ukrainian public in this regard is wide. It is also worth emphasising that such activities will also strengthen the identity of the participants in communication from Ukraine, as a person's perception of themselves as a member of a community that defends its information sovereignty and debunks false narratives about their country is a powerful factor in individual and collective self-identification.

Conclusions

The cyberspace, which emerged due to the digitalisation of the global information space, is the newest space for interaction between peoples and countries. Diplomatic communications within its framework, apart from classic intergovernmental ones, are also public diplomatic and can substantially affect the image of the state through its perception by the public of other countries. Using media resources, social networks, against the backdrop of the cyberneticisation of the information and communication environment, this creates fundamentally new conditions for confrontation between adversary states in the cyber domain and poses enormous challenges to the policy of deterrence. In authoritarian countries, the achievements of the information age were used by media technologies to manipulate the minds of the masses to promote certain ideas and form beliefs in the interests of political power. Among these countries were the Russian Federation, which pursues an aggressive expansionist policy. One of its manifestations is anti-Ukrainian information activities. The false Russian narratives spread around the world, which create a negative image of Ukraine, its government, and the socio-cultural environment overall, are aimed at undermining Ukraine's international authority, slowing down and stopping aid from Western allies. Ukraine must actively counteract the hostile

narratives of the aggressor country in international cyberspace, with Ukrainian cyberdiplomacy in its public and diplomatic format being an effective tool. Specifically, citizen/civil diplomacy. The necessary legal and regulatory framework was in place and relevant changes to Ukrainian legislation are underway. Based on the insufficiency of using only journalism and human resources of state specialised structures to counter Russian hostile information influences on a large scale, as well as on theoretical provisions on citizen/civil diplomacy as a type of public diplomacy, in the context of cyberdiplomacy, the protection of Ukraine's information interests can be carried out using citizen/civil diplomacy tools with the involvement of Ukrainian scientists, politicians, students, and the general public. Among the effective measures is the organisation of multichannel media platforms, websites with relevant informational or educational content available to foreign recipients in their languages.

Prospects for further development of the research topic are related to the study and borrowing by Ukraine of international best practices in the field of cyberdiplomacy as a tool to repel information aggression against the country and the study of Ukraine's branding using cyberdiplomacy in the context of countering Russian information invasion.

Acknowledgements

None.

Conflict of Interest

None.

References

[1] Alekseenko, I.V. (2022). Public diplomacy in globalization conditions: New challenges. *Public Administration: Improvement and Development*, 12. doi: 10.32702/2307-2156.2022.12.2.

[2] Al-Muftah, H., Weerakkody, V., Rana, N.P., Sivarajah, U., & Irani, Z. (2018). Factors influencing e-diplomacy implementation: Exploring causal relationships using interpretive structural modelling. *Government Information Quarterly*, 35(3), 502-514. doi: 10.1016/j.giq.2018.03.002.

[3] At Lviv University, we talked about digital diplomacy. (2023). *Information and analytics agency "Gal-info"*. Retrieved from http://surl.li/izuiog.

[4] Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs*, 3(4-5), 353-364. doi: 10.1080/23340460.2017.1414924.

[5] Bortniak, V., Drozd, O., Zhuravlyov, D., Kopotun, I., Koropatnik, I., Pietkov, V., Pietkov, S., Siedykh, Yu., & Sharashenidze, A. (2022). *People's diplomacy during the war in Ukraine. History, current state, main directions of implementation, real examples*. Kyiv: Professional Publishing House.

[6] Constitution of Ukraine. (1996, June). Retrieved from https://www.president.gov.ua/documents/constitution.

[7] Danilyan, O., & Dzoban, O. (2022). Information war in the media space of modern society. *Bulletin of Yaroslav Mudryi National Law University. Series: Philosophy, Philosophy of Law, Political Science, Sociology*, 3(54), 11-29. doi: 10.21564/2663-5704.54.265589.

[8] Decree of the of the President of Ukraine No. 685/2021 "On the Decision of the National Security and Defence Council of Ukraine of 15 October 2021 "On the Information Security Strategy". (2021, December). Retrieved from https://zakon.rada.gov.ua/laws/show/685/2021#Text.

[9] Decree of the President of Ukraine No. 447/2021 "On the Decision of the National Security" and Defence Council of Ukraine "On the Cybersecurity Strategy of Ukraine". (2021, May). Retrieved from https://www.president.gov.ua/documents/4472021-40013.

[10] Demianenko, M. (2018). Countering information aggression: World experience and domestic realities. *Scientific Works of the Vernadsky National Library of Ukraine*, 50, 225-240. doi: 10.15407/np.50.225.

[11] Deputy Minister: MFA is developing Ukraine's cyber diplomacy strategy. (2024). *UkrInform*. Retrieved from http://surl.li/xjhpnw.

[12] Draft Council Conclusions on Cyber Diplomacy 6122/15. (2015, February). *Council of the European Union*. Retrieved from https://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf.

[13] Dubov, D. (2014). *Cyberspace as a new dimension of geopolitical rivalry*. Kyiv: NISS.

[14] Dzerkal, V. (2023). Tools of cyber diplomacy in the implementation of the state's foreign policy. In *Proceedings of the international scientific and practical conference. Actual problems of modern international relations* (pp. 198-200). Dnipro: PrintDim.

[15] Dzhus, O. (2022). Conceptual foundations of information war in the modern conditions of the armed aggression of the Russian Federation against Ukraine. *Politology Bulletin*, 88, 189-201. doi: 10.17721/2415-881x.2022.88.189-201.

[16] Holovko, I. (2022). New public diplomacy in the modern scientific discourse. *Philosophy and Political Science in the Context of Modern Culture*, 14(2), 102-109. doi: 10.15421/352228.

[17] Ilnytskyj, V., Starka, V., & Haliv, M. (2022). Russian propaganda as an element of preparation for armed

aggression against Ukraine. *Ukrainian Historical Journal*, 5, 43-55. doi: 10.15407/uhj2022.05.043.
[18] Komar, O. (2022). Soft power and propaganda in the Russian-Ukrainian war: Epistemological analysis. *Ukrainian Almanac*, 30, 82-88. doi: 10.17721/2520-2626/2022.30.11.
[19] Kovalskyi, S. (2023). Countering Russian disinformation and propaganda in the Ukrainian information space (on the example of the electronic resource of the Center for Countering Disinformation at the NSDC of Ukraine). *Dialogue: Media Studios*, 29, 96-108. doi: 10.18524/2308-3255.2023.29.300638.
[20] Kukalets, O. (2020). Public diplomacy in the theory of international relations. *Scientific Notes of Students and Postgraduates. Series "International Relations"*, 5, 141-147.
[21] Law of Ukraine No. 2163-VII "On the Basic Principles of Ensuring Cybersecurity of Ukraine". (2024, June). Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text.
[22] Lukianchikova, V.Y. (2013). Cyberspace: Threats to international relations and global security. *Gilea: Scientific Bulletin*, 72, 793-796.
[23] Marushchak, A.I. (2022). Prerequisites for the formation of legal mechanisms for countering disinformation in social media in the context of national security: Problem statement. *Information And Law*, 1, 82-88.
[24] Matviienko, V., & Petushkova, G. (2024). Cyber diplomacy in the European Union: The Estonian model of cyber diplomacy and Ukraine's experience. *Diplomatic Ukraine*, 24, 696-708. doi: 10.37837/2707-7683-2023-37.
[25] Mikhailovsky, R.A., & Budur, I.M. (2023). The geopolitical dimension of information confrontation. In *Materals of scientific seminar of the Kharkiv National University of the Air Force named after Ivan Kozhedub "Information confrontation in the conditions of the Russian-Ukrainian* war" (pp. 127-132). Kharkiv: KhNUAF named after I. Kozhedub.
[26] NATO Deputy Secretary General 2019-2024. (2024). *North Atlantic Treaty Organization*. Retrieved from https://www.nato.int/cps/en/natohq/who_is_who_167942.htm.
[27] One billion dollars for the war of meaning. The enemy aims at our identity. (2023). *Hromada.Group*. Retrieved from http://surl.li/yanyfe.
[28] Oxford English Dictionary. (2024). *Public diplomacy*. Oxford: Oxford University Press. Retrieved from https://www.oed.com/dictionary/public-diplomacy_n?tab=factsheet#27764860100.
[29] Pasichna, V. (2023). Cyberdiplomacy and its impact on the information society. In *Proceedings of the international scientific conference "Digital diplomacy of Ukraine: Synergy of real and virtual"* (pp. 79-81). Lviv: Ivan Franko National University of Lviv.
[30] Piddubna, L. (2016). Cyberspace as a socio-cultural factor of the network society. *Gilea: Scientific Bulletin,* 105, 204-207.
[31] Pronoza, I. (2020). Mass media and communication in the information war as a modern political practice. *Politikus*, 3, 65-70.
[32] Public Diplomacy Strategy of the Ministry of Foreign Affairs of Ukraine for 2021-2025. (2021). *Ministry of Foreign Affairs of Ukraine*. Retrieved from http://surl.li/cxwuug.
[33] Romtsiv, O., & Kharchenko, A. (2023). Methods of Russian information propaganda and their impact on the image of Ukraine in the world. *Analytical and Comparative Jurisprudence*, 5, 190-193. doi: 10.24144/2788-6018.2023.05.32
[34] Savchuk, A. (2015). Peter Pomerantsev: The goal of Russian propaganda is that no one should trust anyone. *Ukrainian Truth*. Retrieved from http://www.pravda.com.ua/articles/2015/03/31/7063251/.
[35] Sukhorolska, I. (2022). Public diplomacy in contemporary international relations: New trends and features. *Regional Studies*, 30, 103-107. doi: 10.32782/2663-6170/2022.30.17.
[36] Sukhorolska, I., & Klymchuk, I. (2022). Public diplomacy under the conditions of Russia's aggressive war against Ukraine. *Bulletin of Lviv University. Serie "Philosophical and Political Studies"*, 43, 322-331 https://doi.org/10.30970/PPS.2022.43.39).
[37] Sunhurova, S. (2022). International experience of struggling with the political violence by means of information warfare. *Politology Bulletin*, 88, 202-218. doi: 10.17721/2415–88IX.2022.88.202-218.
[38] Sviderska, O. (2022). Digital propaganda and information security risks in the context of the Russian-Ukrainian war. *Politikus*, 2, 60-65. doi: 10.24195/2414- 9616.2022-2.10.
[39] Tarasiuk, A. (2019). Correlation of information and cyber security. *Information and Law*, 4, 73-82. doi: 10.37750/2616-6798.2019.4(31).194721.
[40] Trofymenko, M.V. (2023). Transformation of public diplomacy in the context of globalisation and digitalisation: Methodological principles and practical aspects (Ukrainian case). *Bulletin of Mariupol State University. Series: History. Political Studies,* 35-36, 141-154. doi: 10.34079/2226-2830-2023-13-35-36-141-154.
[41] Tsivaty, V. (2023). Digital diplomacy of Ukraine: Innovative, security and international political discourses (synergy of real and virtual). In *Proceedings of the international scientific conference "Digital diplomacy of*

Ukraine: Synergy of real and virtual (pp. 108-112). Lviv: Ivan Franko National University of Lviv.
[42] Ukraine is offered cyberdiplomacy. (2024). *ZN,UA*. Retrieved from https://zn.ua/ukr/UKRAINE/ukrajini-proponujut-kiberdiplomatiju.html.
[43] Vashchenko, N. (2020). The main narratives of Russian propoganda as impact-generating issues in terms of consciental war of Russia against Ukraine. *Scientific Notes of Institute of Journalism*, 1, 180-201. doi: 10.17721/2522-1272.2020.76.15.
[44] Verkhovtseva, I. (2023). Cooperation of local self-government bodies of Ukraine with European partners under conditions of war 2022-2023: Public-diplomatic dimension (organizational-legal aspects). In *New agenda for Europe and the European Union: Reasons - directions - priority goals* (pp. 18-26). Lviv-Olshtyn: Publishing House of Lviv Polytechnic.
[45] Yakovenko, N., & Piskorska, G. (2018). Transformation of NATO public diplomacy. *American History and Politics*, 5, 197-206. doi: 10.17721/2521-1706.2018.05.197-206.
[46] Yemets, V. (2023). Public diplomacy as a tool for forming image of Ukraine in the condition of full-scale war. *Bulletin of Lviv University. Philosophical and Political Studies*, 46, 291-296. doi: 10.30970/PPS.2023.46.36.
[47] Zelenko, H. (Ed.). (2024). *Fake Russia: Imitation of greatness and power*. Nizhyn: Lysenko MM.

Кібердипломатія України у протидії російській інформаційній агресії

Ірина Верховцева
Доктор історичних наук, доцент
Державний університет інформаційно-комунікаційних технологій
03110, вул. Солом'янська, 7, м. Київ, Україна
https://orcid.org/0000-0002-5682-993X

Анотація. Протидія України інформаційній агресії Росії на міжнародній арені після початку її інтервенції в 2014 році у Донеччині, Луганщині, Криму з метою дискредитації всього українського зумовила пошук ефективних інструментів з урахуванням інтенсифікації процесів у кіберпросторі та глобалізації комунікацій. Метою роботи було довести, що одним з ефективних інструментів протидії України російській інформаційній агресії антиукраїнського характеру в міжнародних комунікаціях є кібердипломатія в її публічно-дипломатичному форматі. Методологія дослідження включала набір загальнонаукових методів (логіка, індукція, дедукція, аналіз, синтез) та спеціалізованих методів, таких як структурно-функціональний, типологічний, наративний методи та метод узагальнення. Революція інформаційно-комунікаційних технологій та кібернетизація глобального інформаційного поля з 1980-х формують нову реальність – кіберпростір. Як комунікативне середовище в публічно-дипломатичних практиках, він суттєво впливав на комунікацію урядів з громадськістю зарубіжних країн з метою впливу на іноземні уряди засобом просування національних ідей, цінностей, інститутів, культури, політик у інформаційному полі цільової аудиторії, що впливає на імідж держави через її сприйняття зарубіжною громадськістю. У цьому контексті агресивна політика Російської Федерації з опорою на здобутки інформаційної епохи продемонструвала, як авторитарні країни маніпулюють свідомістю людей і формують вигідні їм переконання. Зокрема, антиукраїнська інформаційна діяльність та поширення світом неправдивих наративів формує негативний імідж України, аби підірвати її міжнародний авторитет, загальмувати допомогу Західного світу. Україна має активно протидіяти цим ворожим наративам у рамках міжнародного кіберпростору, ефективним засобом чого є кібердипломатія в її публічно-дипломатичному форматі, а одним з інструментів – громадська/народна дипломатія із залученням науковців, політиків, студентства, громадськості та створенням мультиканальних медіаплатформ, де розміщуватимуться інформаційні матеріали відповідного змісту та контент просвітницького характеру із відкритим доступом для адресатів іноземних країн їх мовами. У аспекті практичної цінності результати дослідження слугуватимуть розробленню оптимальних моделей української кібердипломатії

Ключові слова: російська інформаційна війна; дипломатія; публічна дипломатія; комунікації у кіберпросторі; громадська/народна дипломатія