DOI https://doi.org/10.30525/978-9934-26-571-6-22

MASS COMMUNICATION DIMENSION OF INFORMATION VIOLENCE IN CYBERSPACE: TOWARDS INSTITUTIONALISATION OF UKRAINE'S COUNTERACTION (ASPECT OF CYBER DIPLOMACY)

Petkun S. M., Verkhovtseva I. H.

INTRODUCTION

The latest digital means of transmitting information, which have been in the trend of technological change in recent decades, have had a qualitative impact on the communication space by significantly increasing the speed and volume of information circulating in the information environment, as well as by making it easily accessible to users of digital services. This also leads to extremely rapid changes in humanitarian practices, as it has given rise to new forms of mass information influence and can help form the basis for manipulating the mass consciousness. All of this requires special attention to cyberspace, the newest space of communication both within the country and between peoples and countries in the global environment of interaction.

For Ukraine, which is fighting for its right to sovereign and independent existence in the confrontation with the Russian aggressor and defending the values of the Western world and global democracy on the border with the world of Asian autocracies, this poses new challenges related to the protection of its information space from Russian aggressive influences. They have been actively unfolding since 2014, along with the intervention of the Russian Federation in Donetsk, Luhansk, and Crimea, and have significantly intensified since the beginning of Russia's full-scale military invasion in February 2022.

Relying on the new technological capabilities of digital media, the aggressor country is spreading destructive propaganda around the world and waging an information war against the Ukrainian state aimed at discrediting everything Ukrainian and artificially transforming Ukrainian identity in a direction favourable to the aggressor. This requires finding effective countermeasures. In terms of ensuring the national security of Ukraine and developing effective state mechanisms to counter these destructive mass media influences, the issue of institutionalising such activities is extremely relevant. One of the current trends, the emergence of which is due to the very fact of cyber practices in interstate relations, and whose impact on all segments of the information and communication space is undeniable, is the newest area of diplomatic practices – cyber diplomacy.

1. Mass information influences of the digital age: information violence in cyberspace as a threat to national security

As researchers point out, human identification in the digital age, with its previously unknown speed and large volumes of information dissemination and accessibility, makes us comprehend such facets of social life that are associated not only with the sacred collective-group or existential-individual, but also with the mass-communication, determined by social and communication processes of a global, universal scale. A person is identified through his or her involvement in a particular sphere of information, virtual and social spaces. Self-representation of an individual on the Internet is carried out through a nickname, avatar, or page on a social network, due to the freedom of their design and attractiveness to users. The irreversible process of transforming a modern person into Homo digitalis is actively continuing: gadgets have become a commonplace in modern life, the number of mobile operators is increasing, the range of mobile services and functionalities of phones with Internet resources is expanding, and the 'digitisation' of our lives continues[1].

E. Toffler emphasises that there is no longer a stable model of reality. It is changing, and it has to be rethought and reformatted, which leads to greater individualisation, which demassifies the individual and, ultimately, culture. This affects self-identity, which contributes to the constant self-improvement of the individual or, conversely, to regression and incompetence. Unified and standardised work is a thing of the past. Civilisational diversity contributes to the differentiation of technologies and the increasing role of information circulation on the path to global transformation. In such a world, people become less or even completely unpredictable, more individualised and demassified, which complicates their interaction. However, this is only the first signal of social transformations fuelled by the new infosphere. Technological advances and the demassification of the media will change social memory. E. Toffler believes that social demassification is becoming more and more frequent – it is becoming a counterweight to massification, instead contributing to the clustering and sparseness of individuals and their social ties, which is most noticeable in network communication[2]. Content personalisation is aimed at obtaining unique, high-quality or categorised

[1] Требін М.П. Феномен інформаційної війни у світі, що глобалізується. Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія. 2013. № 2. С. 193–194.; Требін М.П. Цифрове суспільство: спроба проникнення в сутність. Цифрова епоха: міждисциплінарний дискурс: монографія. Харків: Право, 2024. С. 9–23.; Требін М.П. Цифровізація як мегатренд сучасного бутя. Цифрова епоха: міждисциплінарний дискурс: монографія. Харків: Право, 2024. С. 31–38, 41–49.

[2] Іщук Н.М. Демасифікація як соціальна трансформація: прогнози та реалії. Актуальні питання масової комунікації. К., 2013. Вип. 14. С. 16–17.

information in a certain format of its consumption (electronic or printed version), which is usually a paid service. Advanced world mass media and network media demonstrate a high level of information and navigation personalisation of personal information and communication flows, creating unique resources with individual navigation capabilities. But such processes have not only positive but also negative consequences[3].

Reality shows that a modern existentially active person in a digital society spends a significant part of their time in a virtual environment. Virtual reality is a computer-generated three-dimensional model of reality that creates the effect of a person's presence in it, allows interaction with the objects presented in it, including new ways of interaction: changing the shape of an object, free movement between micro and macro levels of space, movement of space itself, etc.

Thanks to virtual reality, the primordial human desire to create alternative worlds, which had remained unrealised for so long, has been 'materialised' without compromising the real world in the computer industry. With regard to computers, virtual reality is inextricably linked to graphic technologies, which, through feedback-enabled human-computer interaction, give the effect of being present in an artificial world that is different from the real one. A person immerses himself in this world and begins to consider it more real than reality itself, and most importantly, more attractive to a person, where he can create not only 'reality' but himself in this reality.

Virtual reality attracts people with its freedom, informality, ease of access, lack of need to establish real social relations, brightness and attractiveness of the media form, and a variety of possibilities. The electronic existence of a modern person is gradually becoming attributive, significant in terms of worldview, social and even sense of life. At the same time, it may not be oriented towards the search for meaning and significance, but rather it is aimed at liberation from meanings, imperatives, paradigms in the spirit of postmodernism, focusing on multiplicity, play, individualism and constant choice. In this regard, digital society makes it possible to accelerate the processes associated with human activity, sometimes bringing them to their maximum (love and friendship, creativity, enrichment, consumption of various goods, etc.) Digital existence is qualitatively changing the way we used to live, and for the new generation, life without virtual reality seems impossible. The old man spent many years studying, striving to have a family,

[3] Іщук Н.М. Персоналізація інформації в мережевій комунікації: переваги та недоліки. Наукові записки Інституту журналістики. К., 2015. Т. 58. С. 136–137.

accumulate wealth, fulfil his duty in work or defence, and perhaps even become famous[4].

Information aggression has become a reality of modern life. A modern person is exposed to it hundreds of times every day – the Internet, radio, television, newspapers and magazines impose their understanding of life, which, through its manipulative effect, also affects the worldview of the target audience. However, the main goal of information aggression is not only to influence the consciousness, but also the subconscious, in order to 'correct' public opinion in both the victim and the aggressor countries. The processes of manipulating the mass and individual consciousness with the help of the media, especially electronic media, through information aggression are becoming widespread.

The following main properties of information aggression are distinguished: non-violent nature (through mass media); speed of spread; pandemic nature, indirect nature and secrecy of influence (information impact is global and, unlike physical impact, can be completely invisible); virtual nature of the impact (fragility of the information world, ease of access, possibility of hacking information systems).

According to researchers, the influence of mass communication in modern conditions on the human personality, its self-understanding, is often a manifestation of information violence, mainly through the manipulation of public consciousness in a certain direction. For cyberspace, the protocols for the interaction of systems and their elements are programming languages, network protocols and agreements. One of the most common technologies of mass communication influence in modern conditions, which aims to change the consciousness of people, is propaganda. In international communications, it is carried out by all actors of global political processes, using propaganda influences to one degree or another to ensure their own political goals and interests. In particular, widely used soft power technologies, which are legitimised in international relations and are considered quite suitable for promoting a country's interests in the world, often contain elements of propaganda, spreading information about their country, its culture, attractive tourist or other characteristics among the public of other states. Such manifestations of propaganda influence, as a rule, do not carry a negative semantic load, while their impact on the public consciousness of a foreign

[4] Требін М.П. Феномен інформаційної війни у світі, що глобалізується. Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія. 2013. № 2. С. 190–195.; Требін М.П. Цифрове суспільство: спроба проникнення в сутність. Цифрова епоха: міждисциплінарний дискурс: монографія. Харків: Право, 2024. С. 9–23.; Требін М.П. Цифровізація як мегатренд сучасного бутя. Цифрова епоха: міждисциплінарний дискурс: монографія. Харків: Право, 2024. С. 31–38, 41–49.

country in order to influence its government in the desired direction is not concealed by the generator of propaganda content. Such influence may contain a small degree of information violence or not at all. Instead, in cases where information influence in such a context determines a radical change in the addressee's train of thought, his or her perceptions of a particular phenomenon and levelling his or her assessments in the direction desired by the addressee, then mass media influence should be considered as information violence rather than as a proposal for voluntary acceptance/rejection of the proposed information, including propaganda, content.

Information violence as a component of social violence and a non-violent influence (action) on the mental sphere that contradicts the natural course of events and imperceptibly, by imposing one's own beliefs or distorted information on the opponent, directly involves information interaction and changes the nature of social communications in terms of asymmetric relations. Information violence affects the spiritual and psychological structure of the individual through propaganda and other technologies produced by the media. Emotions, primarily fear, as well as those caused by the use of information violence, are as powerful regulators of human behaviour as the threat of direct physical violence. In view of this, scientists believe that in the current conditions of humanity's transition to a new way of receiving information and changes in the type of consciousness and thinking under the influence of the media, information violence is approaching the means of intangible terrorist activity[5].

According to the authors of the monograph 'Information Age Wars: Interdisciplinary Discourse' (2021), 'the information "battlefield" in both cyberspace and social space is the protocols of information and logical connection of their elements, as well as the means and technologies for their practical implementation. For cyberspace, the protocols for the interaction of systems and their elements are programming languages, network protocols and agreements. The main means of their unauthorised correction are software bookmarks with undeclared capabilities, computer viruses, traffic interception tools and technologies for influencing telecommunications channels. For the social space, the protocol of information and logical interaction is the natural language of the population. And the main means of adjusting the protocols of the social space is now the media[6].

[5] Верховцева І.Г. Російська інформаційна війна проти України 2014–2024 рр. як предмет наукових студій: концепт «інформаційне насильство». Образ. *2024. № 2(45)*. С. 28–32.

[6] Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В.А. Кротюка. Харків: ФОП Федорко М.Ю., 2021. С. 30.

Most researchers consider information violence and all its manifestations in the context of information wars as a special form of international confrontation, which, although historically existing since ancient times, has acquired specific characteristics in the context of digitalisation and the spread of modern communication technologies. As O. Kharytonenko and O. Kharchuk point out, the use of coercive tactics through intimidation gives grounds for the use of the term 'information terrorism', whatever its[7].

Etymologically, the term is primarily related to the Latin 'terror', which means 'to intimidate'. Accordingly, information terrorism is understood as the commission or threat of commission of generally dangerous acts with the use of information technologies and/or information weapons that may cause death or other serious consequences and are aimed at intimidating the population in order to induce a state, international organisation, individual or legal entity or group of individuals to perform or refrain from performing any action. Within information terrorism, psychological and cyber terrorism are distinguished. Psychological terrorism is carried out in the field of political, philosophical, legal, aesthetic, religious and other views and ideas, i.e. in the spiritual sphere, where there is a struggle of ideas. It is usually implemented through the media and has a destructive impact on the general population[8].

I. Rulov emphasises in this vein that the concept of terrorism includes not only terrorist crimes, but also other acts that facilitate them, and in fact corresponds to the category of 'terrorist activity', which means a set of actions to organise, lead, resource and facilitate the functioning of criminal associations of a terrorist nature, as well as the preparation and commission of terrorist acts and other crimes for terrorist purposes[9].

O. Zhayvoronok, O. Kurban, T. Smachylo and A. Kryvtsun point out that in the format of international terrorism, violence for the purpose of intimidation by individuals or non-governmental organisations is aimed at the government, individual government officials or representatives of society, systems that ensure the normal life of the population. The goal is to achieve the development of events desired by terrorists – revolution, destabilisation of society, outbreak of war with another state, independence of a certain territory, decline in the prestige of the government, political changes in the government, etc. with a selection of ideological guidelines and directions of communication processes used to achieve the goal formulated in the mission. The basis of

[7] Харитоненко О.І., Харчук О.В. Визначення, види, актуальні напрямки дослідження інформаційних війн. Гібридна війна і журналістика проблеми інформаційної безпеки / за заг. ред. В. О. Жадька. К.: Вид-во НПУ імені М.П. Драгоманова, 2018. С. 28–63.

[8] Мельник Д.С., Леонов Б.Д. Інформаційний тероризм як загроза національній інформаційній інфраструктурі. Інформація і право. 2024. № 3(50). С. 99–107.

[9] Рульов І. Співвідношення кібертероризму та кіберзлочину. Юридичний вісник. 2021. № 3. С. 179–182.

information terrorism is manipulation of the consciousness of the masses, spreading the information and emotional effect that most terrorist acts are designed to produce, attracting supporters among members of society, influencing the governmental structures that make political decisions, etc. In general, information terrorism is a set of information wars and special operations related to national or transnational criminal structures and special services of foreign countries. The most effective and cheapest instruments of terrorism that are actively used are the global media and the Internet. In combination, they form an information field where reality is presented in a distorted form that turns people's moods in a slightly different direction and enables the terrorist side to sway the public's views in its favour. First and foremost, information terrorism is used to disinform, disorient and profane in order to misperceive, misunderstand and inadequately behave in society. At the international level, in the absence of any universal instruments imposing a direct obligation to adopt legislation specifically targeting information terrorism, most governments prefer to combat such threats using a mixed approach, using a combination of general criminal law and legislation on cybercrime and terrorism. In a number of states, for example, criminal legislation focuses on the main offences without differentiating them by the specific means by which they are committed. According to this approach, the information space is seen only as a means by which terrorists commit crimes, often defined in the provisions of the national criminal code[10].

In view of all this, Russia's hybrid aggression against Ukraine, which began in 2014, and whose anti-Ukrainian information activities (propaganda, information manipulation, disinformation, fakes) became a part of the whole complex of forceful actions, in our opinion, fully corresponds to the concepts of "information violence" and "information terrorism", since, in addition to hostile information influences of a destructive nature, it aims to change the identity of Ukrainians, to reconstruct and "recode" Ukrainian society as a whole[11].

---

[10] Жайворонок О.І. Міжнародний досвід протидії інформаційному тероризму та його імплементація в Україні. Публічне управління та митне адміністрування. 2020. № 1(24). С. 92–95.; Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ: ВІКНУ, 2016. С. 71.; Смачило Т.В., Кривцун А.Р. Феномен інформаційного тероризму як загрози міжнародній безпеці. Молодий вчений. 2017. № 11. С. 124–126.

[11] Верховцева І.Г. Інформаційно-комунікаційний сегмент гібридної війни росії проти України 2014–2024 рр.: пропаганда (стан вітчизняних студій). Наукові праці Національної бібліотеки України імені В. І. Вернадського. 2024. Вип. 70. С. 443–445.; Верховцева І.Г. Фейки російської інформаційної війни проти України: деконструюючи «руський мир» та «історичну росію». Україна в умовах російської агресії: виклики та відповіді: монографія / [І.В. Букрєєва, І.Г. Верховцева, В.В. Гулай та ін.]. Харків: Право, 2024. С. 76–78.; Удавана Росія: імітація величі і могутності / Зеленько Г. (кер. проєкту, наук. редактор) та ін. Ніжин: Вид. Лисенко М.М., 2024.; Petkun S., Verkhovtseva I. Hostile Propaganda Of The Digital Age

The information confrontation between different actors (states, non-governmental, economic and other structures), which involves a set of actions to damage the information sphere of a competing party and protect its own information sphere and information security, is called information warfare. This metaphor is currently circulating in the scientific literature and journalism of Ukraine and foreign countries. The objectives of information warfare are to manipulate public opinion and political orientation of the state's population in order to create political tension and a state close to chaos; reduce the level of information support for government and administration, inspire erroneous management decisions; undermine the international authority of the state, its cooperation with other states; change the system of values that determine the way of life and worldview of people; diminish and level the recognised world achievements in science, technology and other fields. They also exaggerate the importance of mistakes, shortcomings, consequences of wrong actions and unqualified government decisions; create preconditions for economic, spiritual or military defeat, loss of will to fight and win; present their way of life as behaviour and worldview of the future that other nations should follow; undermine the morale of the population and, as a result, reduce defence capability and combat potential; and exert other destructive ideological influence.

Information warfare is a phenomenon that originated in ancient times, along with the emergence of human communication and conflict. However, the term itself came into widespread use in the 1960s. It was first used by Canadian political scientist M. McClure and American politician A. Dulles. In particular, the latter, in his book ‘Secret Surrender’, covering the separate negotiations between the United States and Great Britain, on the one hand, and Reichsführer Himmler, on the other, called information warfare intelligence and sabotage actions to undermine the enemy's rear. In modern conditions, due to the relevant revolutionary technological innovations, information warfare has become a phenomenon that requires in-depth study, taking into account the multi-paradigm nature of this phenomenon (experts distinguish between the relevant systemic, psychological, geopolitical, and conflictological paradigms), against computers and networks that support critical infrastructures (energy, communications, financial, transport) and involves the use of various forms and methods aimed at manipulating and controlling information to achieve military, political or social goals, both by

As Information Violence: Ukraine's Response To Russian Information Invasion. *Modern Science: Prospects, Innovations And Technologies*: Scientific Monograph. Part 1. Ryga: Izdevnieciba “Baltija Publishing”, 2024. P. 446–457.

military forces and non-state actors, to change opinions, distort facts and influence public opinion[12].

The American scholar M. Libitsky identified seven forms of information warfare: command and control; intelligence-based; psychological; economic and information; electronic warfare; hacking; cyber. In this context, psychological warfare is understood as the strategic use of psychological and information methods to influence people's behaviour, thoughts, and emotions. In particular, the use of disinformation and manipulation to change the general public's opinion or mood in a certain direction, which is actually information warfare in the narrow sense of the term[13].

Many of the goals of information warfare are achieved by spreading false or distorted information to create chaos, undermine trust in the government or provoke conflicts between nations by means of disinformation, disorientation, introduction of harmful thoughts into the public consciousness, intimidation of the population or opponents, creation of the basis for loyalty to the aggressor, etc. With the development of social media, information warfare has spread to online platforms and involves the creation and operation of fake accounts, false narratives, and the ingraining of divisive content in the minds of the public in order to manipulate public opinion and provoke discord between different groups of people. The factors of successful information influence include the speed and accessibility of information, constant rapid change of news, the use of emotional influence, social networks and algorithms; and the spread of disinformation and fakes. The latter, due to the wide access to information and the possibility of their dissemination through social networks, threatens the truthfulness and reliability of information, thus undermining trust in the media, government, opinion leaders, political and public activists. According to G. Pocheptsov, despite the fact that information does not shoot or explode, it can be very dangerous. In the virtual space, information weapons cause destruction and irreparable consequences and are closely linked to the semantic warfare that takes place in the cognitive space. Both are information and semantic wars designed to change the behaviour of the enemy/opponent, using tools that program this behaviour, significantly reduce the field of choice for action and form an information agenda for decades. The goal is to change people's beliefs and knowledge, which leads to the levelling of the rules by which facts are understood and, accordingly, to new consequences. An example is the information activities of the Russian

[12] Нарис теорії і практики інформаційно-психологічних операцій / Дзюба М.Т., Жарков Я.М., Ольховой І.О., Онищук М.І. Київ: ВІТІ НТУУ "КПІ", 2006. С. 35.; Проноза І.І. Інформаційна війна: сутність та особливості прояву. Актуальні проблеми політики: збірн. наук. праць. 2018. Вип. 61. С. 77–78.

[13] Libicki M. What is Information Warfare, National Defense University. URL: http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html

authorities during the Chechen wars, when the ‘fighters for the freedom of Ichkeria’ of the first war became ‘mujahideen’ in the second war. Thus, the researcher points out, a different version of the semantic matrix was introduced into the information space, based on the model of the world that was in the minds of the recipients of the message. This ‘pulled’ the rest of the components of this matrix, increasing the effectiveness of the impact on the target audience[14].

The word fake means a fake, a forgery, a fraud. Fake is usually understood as one of the tools of information warfare, along with disinformation, deliberate distortion of certain phenomena, facts, events, with the maliciousness of such distortion being carefully concealed in the case of fake. A fake message contains all the signs of a true message, which makes it possible to influence a certain audience through the use of simulacra – cultural or political entities that copy forms, things, meanings that never actually existed. According to O. Saprykin's observations, the following rough classification of fakes is currently used: accidental; created for information warfare; created for commercial purposes; created to increase traffic; created for an unclear purpose. Of course, in the context of information warfare, fakes are a separate, informational weapon used to influence the consciousness and mindset of the target audience in a short or long-term way. If fakes relate to the phenomena of the past and are aimed at changing its perception in the interests of the addressee, then the question should be raised about the correspondence/inconsistency of the information claiming to be fake with scientifically proven facts, processes, phenomena, and thus debunking fake as a pseudo-historical and propaganda narrative.

Russia's hybrid war against Ukraine, launched in 2014, as American researchers J. Dorschner and A. Rach have shown in their analysis, is based on the combined use of military and non-military means with the application of almost the entire range of state tools, including diplomatic, economic, political, social, and informational, respectively. Political sabotage, full-scale military intervention, intimidation, etc. were the components of this war. The aggressor's initial advantages were related to its common past with Ukraine, knowledge of how it functions, its strengths and weaknesses. With the help of diplomatic measures and soft coercion, using the media, the Russian side, seeking to provoke ethnic, religious and social unrest in Ukrainian regions, destabilise them in general, strengthened its influence in their social and political space, supported separatist tendencies, bribing local politicians and

[14] Почепцов Г. Смислові та інформаційні війни. Інформаційне суспільство. 2013. Вип. 18. С. 21–27.; Pocheptsov G. Russian Propaganda Wars: Russia – Ukraine 2022. URL: https://www.academia.edu/95759898/Pocheptsov_G_Russian_propaganda_wars_Russia_Ukraine_2022_https_www_kvak_ee_files_2023_01_Sojateadlane_20_2022_Georgy_Pocheptsov_RUSSIAN_PROPAGANDA_WARS_RUSSIA_UKRAINE_2022_pdf?email_work_card=title

administrations, financing local criminal groups, fuelling local discontent with the functioning of its central government[15].

An important component of such subversive activities has been information invasions, which have been used by the leadership of the aggressor country for more than a decade as an argument in favour of war against Ukraine. In particular, as follows from the Kremlin dictator's interview with American journalist T. Carlson in early February this year, the Russian political establishment is trying to justify its bloody imperial claims to Ukrainian territories by historical experience, in particular, the experience of Russian-Ukrainian relations in the past. In this context, Ukrainian scholars emphasise that the official Russian historical narrative is not discovered in the course of scientific research, but is constructed in the Kremlin's chambers and offices, based on the values and ideals declared by the authorities. It is from there, according to Denysiuk's observations, that imperial anti-Ukrainian narratives are spread on social media, in particular, YouTube channels. These include narratives such as identifying the history of ancient Rus with the history of modern Russia; promoting the project of the so-called 'Novorossia' – the southeastern region of Ukraine, whose history allegedly began with the settlement of 'Russian' ('russki') peasants by the Russian Empire; the conquest of Ukrainian lands by the Muscovy and their incorporation into the Russian Empire in the second half of the seventeenth and seventeenth centuries as a 'reunification' in a 'pan-Russian' state, etc.[16].

Information warfare is a communication technology aimed at influencing the mass consciousness. Information warfare involves the use of two types of weapons: software and hardware, which is the disabling of enemy media, and social and psychological, which is the targeted influence on public opinion. The main features of information warfare include instantaneous deployment, permanence, constant fuelling, the presence of a 'starting point' and a 'snowball effect'. Analysing the considered concepts of information warfare in terms of their suitability for use in the conditions of modern Ukraine, special emphasis should be placed on the names of M. McLuhan, K. Levin, D. Dening and J. Arkila. McLuhan's theory allows us to analyse the peculiarities of the work of individual media in the course of information warfare, while Kurt Lewin's concept allows us to link Ukraine's failures in the information war

[15] Dorschner J. Hybrid War in the Near Abroad. IHS: Jane's Defence Weekly. 2015. Vol. 52. Iss. 10. P. 24–30.; Rácz A. Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist. Helsinki: Ulkopoliittinen Instituutti Utrikespolitiska Institutet; The Finnish Institute Of International Affairs, 2015. P. 87–93.

[16] Верховцева І.Г. Фейки російської інформаційної війни проти України: деконструюючи «руський мир» та «історичну росію». Україна в умовах російської агресії: виклики та відповіді: монографія / [І.В. Букрєєва, І.Г. Верховцева, В.В. Гулай та ін.]. Харків: Право, 2024. С. 82–90.

with the Russian Federation to the discrepancy between the settings of the "gatekeepers" "filters" and the "filters" in the NSDC. The theory of D. Dening offers us a new perspective on information warfare in the modern world as a war of 'offensive' and 'defensive' strategies. Finally, J. Arkila's concept is the most comprehensive and useful from a practical point of view: the laws of interaction between hierarchies and networks, two types of information, and 'preemptive' strikes are three very key factors without which information warfare is impossible[17].

Information warfare is part of the ideological struggle. It does not directly lead to bloodshed or destruction. There are no casualties, no one is deprived of food or shelter. And this gives rise to a dangerously complacent attitude towards it. At the same time, the destruction caused by information wars in public psychology, the psychology of the individual, is quite commensurate in scale and significance, and sometimes exceeds the consequences of armed wars. The most important task of information warfare is to manipulate the masses in order to introduce hostile, harmful ideas and views into the public and individual consciousness; disorientation and disinformation of the masses; weakening of certain beliefs and ways of life; intimidation of one's people with the image of the enemy and intimidation of the enemy with one's power. By means of information warfare, the aggressor seeks to disrupt the exchange of information in the opponent's camp. This war destroys not the population, but the state mechanism.

Today, the following types of information warfare are distinguished: psychological (information-psychological) warfare; cyber warfare; network warfare; ideological warfare; electronic warfare; seizure/conquest of television and radio broadcasting resources to spread disinformation; blocking communication networks; electronic interference with stock exchange operations to create leaks of sensitive information or spread disinformation.

The main tools of information and psychological warfare as a destructive mass media influence are psychological pressure and dissemination of sensitive content; disinformation; propaganda; fakes. Along with disinformation, deliberate distortion of certain phenomena, facts, events, fake news is an instrument of information warfare. In the case of fake news, the maliciousness of the intentional distortion of information is carefully

[17] Радчич С. Философское осмысление феномена современной информационной войны. URL: https://www.academia.edu/82161813/%D0%A4%D0%B8%D0%BB%D0%BE%D1%81%D0%BE%D1%84%D1%81%D0%BA%D0%BE%D0%B5_%D0%BE%D1%81%D0%BC%D1%8B%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D1%84%D0%B5%D0%BD%D0%BE%D0%BC%D0%B5%D0%BD%D0%B0_%D1%81%D0%BE%D0%B2%D1%80%D0%B5%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B2%D0%BE%D0%B9%D0%BD%D1%8B

concealed. A fake message contains all the signs of a true message, which makes it possible to influence a certain audience through the use of simulacra – cultural or political entities that copy forms, things, meanings that never actually existed.

Fakes can be classified as: accidental; created for information warfare; created for commercial purposes; created to increase traffic; created for an unclear purpose. In the context of information warfare, fake news is a separate, informational weapon used to influence the consciousness and mindset of the target audience in a short or long-term way. If fakes relate to the phenomena of the past and are aimed at changing its perception in the interests of the addressee, then the question should be raised about the correspondence/inconsistency of the information claiming to be fake with scientifically proven facts, processes, phenomena, and thus debunking fake as a pseudo-historical and propaganda narrative.

Indicators of potentially dangerous fakes include: no reference to an official source (information is presented without regard to the subject of its production); emotional text designed to provoke a clear reaction; grammatical inconsistency with the original text; one-sided presentation of information or over-expertise in the presentation of material; anonymity of information; little-known electronic resources, etc.

Information and psychological operations are a complex system of influencing the psychological state of target groups, which is a component of information warfare. Under current conditions, such operations are usually used to reduce the enemy's moral and psychological state and spread disinformation through social media and messengers.

According to scholars, mass media, especially in the digital format, are becoming tools of strategic influence in information wars. Specially created narratives aimed at reducing trust in democratic institutions are spread through social media, which is the basis for further information pressure. Modern media and mass communication outlets have become the most powerful element of the mechanism of purposeful construction of political orders, a means of building the connections and relations with the public necessary for the authorities. The information provided by the media is never neutral. It is a manifestation of the attempts of the ruling elites to create an image of reality that they need and that 'justifies' their practical policies, 'packaged' in stereotypical points of view that are favourable to the authorities and bring to the fore only a part of what is really happening.

While democratic states constitutionally guarantee citizens access to information and freedom of speech, which ensures free and fair participation of citizens in political and other social processes, in authoritarian countries, with the help of 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 minds in order to promote the necessary ideas. This is primarily true of the Russian Federation. By hybridising soft power and propaganda, Russian softpower is a continuation of Russian propaganda and a means of implementing aggressive expansionist policies. At the same time, the aggressor country turns the values of Western liberalism inside out, attacking it with its own means[18].

In general, Russia's approach to information confrontation is a global strategy that includes both cyber strikes and information operations against most democratic actors in the world. Its goals are to restore Russian dominance in the post-Soviet/imperial sphere of influence; reduce the influence of Western democratic values, institutions and systems in order to create a polycentric model of the world; and expand Russia's political, economic and military hegemony around the world to strengthen its status as a great power. Danilian, O. & Dzieban, O. point out that the tasks of information weapons used by Russia are becoming a means of mobilizing supporters and expanding spheres of influence in the international arena. At the same time, an important function of information weapons is to create a virtual "picture of the world", an illusory, parallel reality with a transformed system of values, beliefs, attitudes, and ways of behavior. The objects of influence are the mass consciousness of not only the population of the Russian Federation, but also the population of other countries, including Ukraine[19].

The U.S. government has accused Russian citizens and shut down more than 30 Internet domains of a planned campaign to influence the U.S. election. For Ukraine, another component is much more interesting in this context – the Russian operation to manipulate German, French, Italian and British politicians, businessmen, journalists and other influential people. The 277-page FBI dossier describes in detail Russia's plans to win the "hearts and minds" of Europeans. A sharp increase in such activities was noted after February 24, 2022. A separate surge was recorded on the eve of the European Parliament elections held in June this year. The goal of the Kremlin's campaign in Europe is to sow division, discredit the United States and undermine support for Ukraine, "to elicit rational (e.g., 'really, why should we help Ukraine?') and emotional ("Americans are scum") reactions from the audience," according to documents obtained by the FBI.

[18] Комар О. Soft power і пропаганда у російсько-українській війні: епістемологічний аналіз. Українознавчий альманах. 2022. № 30. С. 84–86.

[19] Данильян О. Г., Дзьобань О. П. Інформаційна війна у медіапросторі сучасного суспільства. Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія. 2022. № 3. С. 17–20.

The investigation uncovered a network of Russian-linked websites posing as Western publications, such as "cloned" Internet portals with slightly modified web addresses that disseminated manipulated content and disinformation. The domains contained fakes of Reuters, Der Spiegel, Bild, Le Monde, Le Parisien, Welt, FAZ, Süddeutsche Zeitung, Delfi and others. The content is created using internal discontent in EU countries. Most often, these campaigns took advantage of existing conflicts that were fomented to escalate tensions, increase discontent, and exacerbate the debate. Sometimes they used true information with a single fake element added to it, and sometimes facts were simply distorted, taken out of context, or outright lies were spread.

Today, in the context of Ukraine's confrontation with Russian information aggression, which targets everything Ukrainian – the government, state, society, culture and identity of Ukrainians – it should be noted that long before the military invasion of Ukraine, Russian propagandists were processing the world community in order to present the picture in a light favorable to the aggressor country and find allies for it. Spreading the ideas of Slavic unity and the "Russian world" around the world, the aggressor country uses systems of organizational, propaganda, psychological, and informational influence. The main goals are to discredit the political leadership and command of the Armed Forces of Ukraine, provoking distrust in them; forming an opinion about the spread of racism and ethnic intolerance in Ukraine; convincing the international community of systematic violations of the ceasefire by the Ukrainian authorities and the covert build-up of the Armed Forces of Ukraine along the demarcation line in order to resume active hostilities; creating a negative image of the defense forces by accusing Ukrainian servicemen of committing crimes, etc. Vashchenko, N. eradicates a number of the main Russian narratives hostile to Ukraine: 1) "Ukraine is an unfortunate shadow of Russia"; 2) "Ukraine is an artificial project of the West" ("Ukraine was invented by Poles and Austrians", "Ukrainian language was created artificially", "Ukraine took away other people's lands"); 3) "Crimea, Donbas and southeastern Ukraine are Russia"; 4) "USSR is a powerful empire, Stalin is a hero"; 5) "All Ukrainian nationalists were fascists"; 6) "Ukraine has forgotten about the victory over Nazism"[20].

The researchers emphasize that in order to undermine Ukraine's international authority, create a negative image of Ukraine and prevent large-scale military, economic, and financial assistance from European countries and the United States, Russia artificially creates a negative image of

[20] Ващенко Н. Головні наративи сучасної російської пропаганди як впливогенна проблематика в умовах консцієнтальної війни Росії проти України. Наукові записки інституту журналістики. 2020. № 1(76). С. 189–190.

Ukrainians as “neo-Nazis” and “Banderites,” provides diametrically opposite coverage of war crimes of the Russian army, and raises doubts about national values and the foundations of the Ukrainian state. The methods of such activities include the spread of fakes, disinformation, manipulation in the information space, and manipulation of historical memory, in particular, regarding the historical heritage and origin of Ukraine, the use of linguistic methods and tools, such as labeling “fascist,” “Nazi,” “Ukranian Nazi,” and “neo-Nazi regime in Kyiv,” which unpack the historical memory of terror related to the crimes committed by the Nazi regime in Germany. At the same time, Russia fully utilizes the resources of the media space to aggressively influence the consciousness and subconsciousness of the addressees (target audience), including the public of the world.

Similar narratives, for example, are spread by Russia in Israel's information space. Plohiy, S. and Pomerantsev, R. point out that the Kremlin is trying to pollute the image of Ukraine in the West and generally make the information field in which Ukraine appears dirty. These researchers emphasize that this information war of the Kremlin is a war not only against Ukraine, but also against the whole of Europe. In today's realities, there is a significant information presence of the Russian Federation in the media space of not only the EU, but also the United States and other countries. Provocation of aggravation of contradictions, information and financial support of conflicts in the territories of Western democracies became possible due to the use of the Russian army of fake accounts, Kremlin bots and the unpreparedness of civilized countries for information warfare in social networks[21].

In addition to justifying its aggressive military actions against the Ukrainian people to the international community, Russia systematically and permanently uses media propaganda to destabilize the socio-political situation and strengthen anti-Ukrainian rhetoric. To organize and implement destructive information and psychological operations against Ukraine in the information space, Russian special services are increasingly using the capabilities of IT giants (services and platforms of Google, LLC), whose technical capacities are used to spread disinformation to manipulate Internet users. Google Play and the App Store are used by the Russian Federation to distribute banned mobile applications of companies and organizations that have been sanctioned. YouTube, Twitter, and Facebook are used to disseminate information content of Russian and separatist entities under sanctions. Google Maps is used to change the original names of Ukrainian government agencies and foreign diplomatic missions in Ukraine. At the same

[21] Пітер Померанцев: «Мета російської пропаганди – щоб ніхто нікому не довіряв». URL: http://www.pravda.com.ua/articles/2015/03/31/7063251/

time, the aggressor country uses the Telegram messenger for information operations against the top military and political leadership of the state, propaganda of separatism, dissemination of destructive information, etc. This is facilitated by the impossibility of identifying users, which leads to their avoidance of criminal liability for spreading destructive information. At the same time, the ability to anonymize disseminators is destructively used to create and use communication channels between military and terrorist organizations, as well as as a means of communicating their information messages to a wide range of users.

One of the most powerful instruments of influence on Europeans and people around the world is Russia Today, a multimedia international news agency whose goal is to provide prompt, "Russian-style" coverage of world events, i.e. to tell the international audience about the Russian view of the situation. Russia Today's correspondent network includes more than 40 offices around the world. The agency broadcasts in many languages. According to Liz Wahl, a journalist and former Russia Today TV presenter, based on her own experience, the effectiveness of Russian lies is largely due to the methodology of working with the audience and is similar to a sect that uses psychological influence. No matter how implausible the news is, Russian media manage to make it popular with the help of an army of Internet trolls, paid experts, and powerful funding. However, Russian propaganda in EU countries is very different from that in Russia or Ukraine. Public opinion about Ukraine in Italy, for example, is very divided. Italian "Euro-optimists" support Ukraine's European aspirations (joining the EU and NATO), but Euro-skeptics and businessmen believe that Russia is a much more serious economic market than Ukraine. This is happening against the backdrop of a lack of knowledge about Ukraine and creates favorable conditions for Italy to support Russia's position on Ukraine.

2. Ukraine's counteraction to destructive mass media influences: The potential of cyber diplomacy and the basis for its institutionalization

As Matvienko, V. & Petushkova, G., point out, the main problems in cyberspace are related to the human factor. They are mostly geopolitical. The challenges of cyberspace are about the success of negotiations and political debates on the management of this environment. One of the main problems of cybersecurity in this area is not about how to prevent intrusions, but about the political motivation of individuals and organizations to take responsibility for regulating the components of cybersecurity, as well as how these entities can limit and hold accountable for the malicious activities of an actor in international relations. International law cannot be applied to cyberspace in full and without constant amendments due to the rapid pace of development

of information and communication technologies. Currently, the international community has 11 non-binding norms of responsible behavior of states from a group of UN governmental experts. Most states have their own concepts and strategic plans, which in practice contradict the norms, since they are non-binding. There are inconsistencies at the international and national levels. Classical concepts of international relations, such as neutrality or arms control, do not make sense in cyberspace in their traditional form[22].

It is believed that during the legal regime of martial law, illegal (destructive) content on the Internet and social networks primarily includes propaganda information materials containing calls for the overthrow of the constitutional order and encroachment on the territorial integrity of Ukraine, incitement to national or religious hatred, manifestations of xenophobia, justification of Russian military aggression against Ukraine, glorification of its participants, etc. This category also includes propaganda materials and posts calling for the occupation of Ukraine on social media. This necessitates the development of an organizational and legal framework for countering Russian propaganda, disinformation, fakes, and destructive content. According to this researcher, in Ukraine, state institutions and law enforcement agencies should primarily counteract the large-scale influence of Russian bot farms and troll factories. First of all, through the creation of a single center for countering Russian propaganda on social media, which should combine the activities of government and public organizations. The next step is to widely inform social media users about information "hygiene" and explain the methodology for detecting and identifying Russian trolls. It would also be advisable to create a unified record of identified "creambots" and special programs and applications that would help identify "trolls" among users. Active cooperation with the management of social networks themselves in terms of countering trolls will help to block them quickly. Active counter-propaganda at the state level remains one of the most important tools in the fight against Russian illegal and criminal activity on social media. In such circumstances, the relevance of legal regulation of the content of destructive information in textual information sources is growing. Due to the growing distribution and level of public danger of destructive content of Russian origin, there is an urgent need for appropriate legal regulation and development of effective measures to combat it. However, domestic legislation does not contain a systematic list of criteria on the basis of which it is possible to define destructive information content. The researcher recommends defining clear criteria for understanding and interpreting illegal

[22] Матвієнко В., Петушкова Г. Кібердипломатія в Європейському Союзі: модель естонської кібердипломатії та досвід України. Україна дипломатична. 2024. Вип. XXIV. С. 697–698.

(destructive) content at the legislative level with the possibility of updating them; creating a register by category of destructive content; improving the system of monitoring social networks using the capabilities of artificial intelligence systems and algorithms; and developing a single basic list of requirements and rules for blocking destructive content. In order to form such a list, it is proposed to introduce into domestic legislation the concept of a "destructive indicator" or "indicator of destructive orientation" – a criterion by which the presence of illegal semantics in textual information is searched for, and the identification of which is the basis for classifying information as destructive[23].

Ukraine is taking many effective measures to counteract information aggression. These include information education, fact-checking, information volunteering, cyber diplomacy, etc. Among the government measures to build anti-fake services, various institutions for countering disinformation, which are being created under the relevant departmental authorities, play a significant role. For example, in 2021, the Center for Countering Disinformation was established as a working body of the National Security and Defense Council of Ukraine, which ensures the implementation of measures to counter current and projected threats to national security and national interests of Ukraine in the information sphere, takes care of Ukraine's information security, detects fakes and counteracts disinformation, hostile propaganda, destructive information influences and campaigns, and prevents attempts to manipulate public opinion. The main focus is on countering the spread of false information and combating information terrorism. Another governmental organization dedicated to combating disinformation and harmful information influences is the Center for Strategic Communications and Information Security under the Ministry of Culture and Information Policy of Ukraine, also established in 2021. Its work focuses on countering external threats, combining the efforts of the state and NGOs in combating disinformation, responding quickly to fakes, and promoting Ukrainian narratives.

Effective means of counteracting information influences and information aggression include the activities of fact-checking and analytical centres; monitoring of all media without exception; constant verification of content and sources of information; open communication in the information space; ensuring effective delivery of key messages; work of media with a reliable

[23] Мельніченко О.А. Основні напрями деструктивної діяльності російських спецслужб в інформаційній війні проти України. Гібридна війна: сутність, виклики та загрози: збірн. матер. круглого столу (Київ, 8 липня 2021 р.). Київ: НА СБУ, 2021. С. 31–32.; Савич А.С. Комунікативні інструменти протидії інформаційної агресії Росії: світовий досвід. Вісник Маріупольського державного університету. Серія: Історія. Політологія. 2015. Вип. 12. С. 272–275.

reputation for refuting fake data; systematic counterattacks on fake news; creation of own narratives that promptly refute fakes, etc. At the same time, democratic forms of social organisation are being transformed, as the role of the Internet in the development of democratic processes is fundamentally different from that of traditional media.

Fact-checking (literally, 'fact-checking') involves the process of checking available facts and data to determine their completeness, reliability and truth, and its main goal is to identify discrepancies between facts and reality. Professional verification is mostly carried out by fact-checking agencies (e.g., www.euvsdisinfo.eu) or specialised software products and services (e.g., Google Images, TinEye, Fotoforensics, InVID Project, etc.). In Ukraine, the first fact-checking organisation was the analytical portal Slovo i Dilo (2008), which monitored the correspondence between politicians' promises and their actual actions. Later, the StopFake portal was created (2014) to combat Russian propaganda fakes, as well as analytical platforms and specialised projects such as VoxCheck, FactCheck (2016, since 2018 – BezBrekhni) and others.

On 02 February 2023, Nations Against Disinformation launched a new creative tool to counter disinformation. Ukraine joins the efforts of governments, businesses and civil society around the world to build resilience and counter disinformation. The first joint communication campaign is being launched in partnership between the Ministry of Foreign Affairs of Ukraine, the Ministry of Foreign Affairs of Ukraine, the Ministry of Foreign Affairs of the Republic of Estonia, and EUvsDisinfo, a project of the European External Action Service's Strategic Communications Task Force. 'Nations Against Disinformation' is an initiative aimed at raising awareness of the dangers of disinformation and its serious negative consequences for societies. As part of the initiative, partners are planning joint international campaigns, events, conferences, webinars and workshops to share best practices in countering disinformation.

'Ukraine has a unique experience in countering disinformation, formed over the years of fighting Russian propaganda. This is a powerful added value of our country for the entire Euro-Atlantic community and the world. Today, we are already a global leader in this area, uniting states and organisations in countering disinformation that threatens the lives and security of millions of people. The Nations Against Disinformation initiative has brought together a number of like-minded partners for this very purpose and is open to all those who seek to protect the common information space, promote media literacy and critical thinking.' The European Union recognises disinformation as one of the biggest challenges facing Europe, requiring a coordinated response from all EU member states, online platforms, media and our international partners. This initiative is an excellent example of the combined efforts and

cooperation between countries, governments and non-governmental organisations. In this way, we underline the value of unity in the face of a global threat,' said Matti Maasikas, Head of the EU Delegation to Ukraine.

The Nations Against Disinformation campaign was initiated by the Ministry of Foreign Affairs of Ukraine and the NGO BRAND UKRAINE. The project is co-funded by the EU and the National Democratic Institute. The key goals and principles of partnership within the initiative are presented on the campaign's website. 'Nations Against Disinformation' is launched with an international communication campaign to promote "The Distortion Test". The Distortion Test directly visualises how disinformation distorts reality, remaining invisible and imperceptible to any of the human senses.

Given all this, as well as the globalisation and digitalisation of the information space and cyber threats to international communications, cyber diplomacy has become a response to the information challenges of our time. It is based on the dimensions of soft power and is an effective practice for mitigating uncertainty, eliminating risks and potential conflicts emanating from cyberspace.

O. Vysotskyi was one of the first scholars in the domestic academic field to interpret the term 'cyber diplomacy'. In particular, in 2020, in his lectures, he pointed out that digital diplomacy is a continuation and expansion of public diplomacy, but in a different context of reality, in the global information world of the Internet. In this vein, the researcher pointed out the interchangeability, in his opinion, of the terms 'digital diplomacy' and 'cyber diplomacy' and emphasised the specifics of public diplomatic practices in the context of digitalisation of communications in the global information space, considering cyber diplomacy as one of the segments/variations of public diplomacy[24].

Matvienko, V. & Petushkova, G. focus on the technological aspects of digital diplomacy and a much broader interpretation of cyber diplomacy as a diplomatic practice that applies to cyberspace in general. These researchers define cyber diplomacy at the national level as the use of diplomatic instruments and initiatives to secure the interests of the state in cyberspace. The tasks for a diplomatic agent in this context are as follows: establishing communication and dialogue between state and non-state actors at different levels; preventing cyber warfare; building global norms in cyberspace, etc.

[24] Висоцький О.Ю. Публічна дипломатія: конспект лекцій. Ч. І. Дніпро: СПД «Охотнік», 2020. С. 697–698.; Висоцький О. Iphone-дипломатія президента України в контексті новацій української цифрової дипломатії під час широкомасштабної російської агресії. Україна і світ: теоретичні та практичні аспекти діяльності у сфері міжнародних відносин: матер. Міжнар. наук.-практ. конф., м. Київ, 11–12 квіт. 2024 р. Київ: Вид. центр КНУКіМ, 2024. С. 16–17.; Матвієнко В., Петушкова Г. Кібердипломатія в Європейському Союзі: модель естонської кібердипломатії та досвід України. Україна дипломатична. 2024. Вип. XXIV. С. 702–703.

Given this, cyber diplomacy, as scholars point out, is based on the dimensions of soft power and is an effective practice for mitigating uncertainty, eliminating risks and potential conflicts arising from cyberspace. The fundamental elements of cyber diplomacy are increasing cyber capabilities, building trust, and adherence to and development of cyber norms. This, according to scholars, necessitates a rethinking of the role of diplomats, reorganisation of departments and ministries of foreign affairs in general to meet the growing need for cybersecurity experts in the implementation of foreign policy objectives and rethink the role of new technologies in modern international relations[25].

As we can see, the positions of O. Vysotskyi and V. Matvienko and H. Petushkova do not coincide – from a purely technological interpretation of digital diplomacy as an interchangeable category with cyber diplomacy, we can observe a gradual transition in the visions of domestic scholars to considering cyber diplomacy as a much broader concept than digital diplomacy, to a concept that covers almost all practices of diplomacy in cyberspace.

Western scholarship interprets cyber diplomacy as an art, a science, and at the same time a means by which nations, groups, or individuals conduct their affairs in cyberspace, protecting their interests and promoting their political, economic, cultural, or scientific relations while maintaining peaceful relations. In this context, cyber diplomacy involves the use of diplomatic tools and initiatives to achieve goals in the complex and uncharted territory of cyberspace, which is constantly evolving. States use common and accepted rules, protocols and models of behaviour to facilitate interaction between global public and private sector actors. In this context, cyber diplomacy should minimise the effects of cyber aggressions, cyber attacks on critical infrastructure, data leakage, cybercrime, cyber espionage, online theft and offensive cyber operations carried out by state or non-state actors that increasingly use cyberspace and the Internet for manipulation, disruption, fraud, extortion, data theft, and money laundering. It is noted that cyberattacks such as WannaCry have damaged more than 200,000 computers in 150 countries and cost an estimated $4 billion. As a result, the Internet has become an arena for geopolitical battles and the spread of disinformation. In addition, the political dimension of cyber diplomacy is no less important, as demonstrated repeatedly during the US elections, with cyberattacks against the Macron campaign, the German Bundestag and other parliaments and ministries[26].

[25] Висоцький О.Ю. Публічна дипломатія: конспект лекцій. Ч. І. Дніпро: СПД «Охотнік», 2020. С. 697–698.

[26] What is cyber diplomacy? URL: https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html

G. Christou in his article 'Cyber Diplomacy: From Concept to Practice' emphasises that cyberspace security is both a national and international strategic priority and a necessity for many state and non-state actors seeking to create a reliable, secure and sustainable digital ecosystem of the 21st century. The researcher believes that events and crises such as the COVID-19 pandemic, the war in Ukraine, and the rapid development and use of new technologies have only accelerated these trends, among other things, challenging geopolitical and ideological processes, raising the issue of regulatory differences and disputes between states over how cyberspace should be governed[27].

Another foreign scholar R. Robinson in his publication 'Cyber Diplomacy: A New Frontier in International Relations and Professional Practice, believes that cyber diplomacy should be considered as an equal and important part of a broader and more holistic toolkit of state cybersecurity policy. According to this scholar, cyber diplomacy is a continuation of diplomacy in a broader sense, which itself is a field that has undergone significant changes over the years to adapt to new conditions and address the pressing issues of our time, such as climate change and space within the post-liberal and increasingly chaotic world order, with the expansion and deepening of processes, scales and actors involved, as well as the transformation of diplomacy modalities in the multilateral 2.0 world of the 21st century[28].

Barrinha A. & Renard T. take a similar position. Cyberdiplomacy is defined as diplomacy in cyberspace, or, in other words, the use of diplomatic resources and the exercise of diplomatic functions to secure national interests in cyberspace. At the same time, the dominant issues on the cyber diplomacy agenda are cybersecurity, cybercrime, confidence building, Internet freedom and Internet governance. Thus, cyber diplomacy is carried out, in whole or in part, by diplomats meeting in bilateral formats (e.g., the US-China dialogue) or in multilateral forums (e.g., the UN). Outside of the traditional sphere of diplomacy, diplomats also interact with various non-state actors, such as leaders of internet companies (e.g. Facebook or Google), technology entrepreneurs or civil society organisations. Diplomacy can also include amplifying the voices of the oppressed in other countries through technology. Although this defines a fairly wide range of activities, it allows cyber

[27] Christou G. Cyber Diplomacy: From Concept to Practice. Tallinn Paper. 2024. No. 14. URL: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf

[28] Robinson R. Cyber Diplomacy: A New Frontier in International Relations and Professional Practice. EDRM. URL: https://edrm.net/2024/06/cyber-diplomacy-a-new-frontier-in-international-relations-and-professional-practice/; Barrinha A., Renard T. (2017). Cyber-diplomacy: The making of an international society in the digital age. Global Affairs, 3(4-5), 353–364.

diplomacy to be firmly positioned as an international social institution, even when interacting with actors in the global society[29].

Thus, according to most researchers, both domestic and Western, cyber diplomacy is a much broader concept than digital diplomacy. The latter focuses purely on the technological aspects of communication practices in public diplomacy. Cyber diplomacy, on the other hand, includes the entire range of diplomatic activities and is carried out in cyberspace. At the same time, cyber diplomacy has both a technological dimension and a purely public diplomatic one, related to the relevant social communications.

The starting point of cyber diplomacy is considered to be the publication in 2011 of the US International Strategy for Cyberspace, which was the first government document in the world to focus entirely on the international aspects of cyberspace and rely 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, as well as a call to the private sector, civil society, and end users to strengthen efforts through partnership, awareness, and action to achieve the future we all share. The Strategy set out the following goals: coordinating the Department's global diplomatic activities on cybersecurity; ensuring the Department's liaison with the White House and federal ministries and agencies on these issues; advising government officials on cybersecurity; establishing communication with public and private organisations on cybersecurity; and coordinating the work of the Department's regional and functional bureaus dealing with these areas. To implement the Strategy, the Office of the Coordinator for Cyber Issues was established, which is fully dedicated to cyber issues in the foreign policy dimension[30].

The web of cyber diplomacy is expanding and deepening at a rapid pace, gradually creating a cyber international society. There is a growing challenge in the global community to attribute cyberattacks, and a small fear of escalation between actors due to the unforeseen consequences of cybercrime. The international community aims to expand the effect of cyberspace governance from regional and national initiatives to a global unified approach. The relevant diplomatic services in different countries use Internet platforms to communicate directly with the target audience of a foreign country,

[29] Christou G. Cyber Diplomacy: From Concept to Practice. Tallinn Paper. 2024. No. 14. URL: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf

[30] Пасічна В. Кібердипломатія та її вплив на інформаційне суспільство. Цифрова дипломатія України: синергія реального і віртуального. Матеріали міжнародної наукової конференції. Львів, 24 листопада 2023 р. / Упорядники: М. Мальський, Р. Вовк, О. Кучик. Львів: ЛНУ імені Івана Франка, 2023. С. 79–80.

disseminate important information among foreign citizens and conduct social surveys[31]. For successful cyber diplomacy, it is important to monitor and analyse information using analytics tools to track reactions to their actions and develop communication strategies. The effective use of social media and other e-diplomacy tools increases the effectiveness of work in the international arena, raises the authority of the state and diplomat, improves the image of political leaders, attracts supporters and influences opponents. Of equal importance is the fact that social media can become a basis for conflict resolution[32].

In 2013, the European Union's external cyber coordination leadership noted in the context of EU cyberspace coordination that today 'there are very few countries where national cyber coordination is effective and the state is able to speak with one voice in all international fora. Less than a decade ago, diplomats were called upon to regulate cyberspace, which until then had remained outside the realm of diplomacy. Instead, the situation is changing, and the number of cyber diplomats involved in bilateral and multilateral contacts at all levels around the world is steadily growing. In 2015. The EU recognised the critical importance of further developing and implementing the EU's comprehensive approach to cyber diplomacy at the global level and stressed the compliance in this area with the EU's fundamental values, such as democracy, human rights, the rule of law, including the right to freedom of expression, access to information and the right to privacy, ensuring that the Internet is not used to incite hatred and violence and remains, with strict respect for fundamental freedoms, a forum for free and open discussion and exchange of information. The EU's objectives in this area include enabling citizens to access information that will allow them to fully enjoy the social, cultural and economic benefits of cyberspace, including by promoting the creation of more secure digital infrastructures[33].

In recent years, the North Atlantic Alliance has significantly intensified its communication activities within the framework of public diplomacy. It uses online media, social media platforms, etc. to engage in discussions on security issues. In this context, considerable attention is paid to technologies,

[31] Дзеркаль В. Інструменти кібер-дипломатії у реалізації зовнішньої політики держави. Актуальні проблеми сучасних міжнародних відносин. Матеріали Всеукраїнської науково-практичної конференції. 17-18 листопада 2023 р., м. Дніпро. / ред. кол.: І.В. Іщенко, І.К. Головко, П.Г. Петров. Дніпро: ПрінтДім, 2023. С. 198–199.

[32] Al-Muftah, H., Weerakkody, V., Rana, N.P., Sivarajah, U., & Irani, Z. (2018). Factors 200 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

[33] 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

information weapons, propaganda operations in the wars of the 21st century, and the importance of strengthening cyber defence and resilience at all levels is given due recognition. In 2016, NATO recognised cyberspace as an operational domain, alongside land and sea, which launched the Alliance's efforts to strengthen its cyber defences. A new comprehensive cyber defence policy followed in June 2021, recognising that cyberspace is always subject to competition. In this regard, NATO convened the first-ever North Atlantic Cyber Coordinators Council. At the same time, cyber diplomacy in the NATO armed forces, especially in the United States, has significantly changed the attitude of key players to the geopolitical and civilisational confrontation. This was highlighted in May 2022 at the first International Conference on Cyber Diplomacy 'Building Global Digitalisation: Building Trust and Security through Cyber Diplomacy', organised by the National Institute for Research and Development of Informatics in Bucharest in partnership with the Romanian Ministry of Foreign Affairs. The event brought together ambassadors, academics, experts from the international cyber and defence community and aimed 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[34].

In addition to the important potential of cyber diplomacy given the current conditions of development of information and communication technologies on a global scale, the role that this diplomatic tool can play in organising counteraction to information aggression against a particular country is equally important.

Anti-Ukrainian narratives, for example, spread by Russia in the Israeli information space, indicate 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[35]. These researchers emphasise that this Kremlin's information war is a war not only against Ukraine, but also against the whole of Europe. Scholars believe that the Russian terrorist attack on the infrastructure of the mind requires extraordinary methods. Journalism methods are not enough in this context – it cannot do it alone. In the same

[34] Дем'яненко М. Протидія інформаційній агресії: світовий досвід та вітчизняні реалії. Наукові праці Національної бібліотеки України імені В. І. Вернадського. 2018. № 50. С. 227–231.; Deputy Secretary General Opens First International Conference on Cyber Diplomacy, Building Global Digitalization (2022). Retrieved from https://www.nato.int/cps/en/natohq/news_195445.htm

[35] Росія поширює в Ізраїлі фейки про Україну на «популярних сайтах». URL: https://www.ukrinform.ua/rubric-world/3738744-rosia-posirue-v-izraili-fejki-pro-ukrainu-na-popularnih-sajtah-zmi.html; Сергій Плохій: «Ця війна є війною за всю Європу». URL: https://zbruc.eu/node/110984; Пітер Померанцев: «Мета російської пропаганди – щоб ніхто нікому не довіряв». URL: http://www.pravda.com.ua/articles/2015/03/31/7063251/

vein, Danilian, & Dzieban, (2022) agree that traditional methods of combating information attacks on social media do not produce the desired results[36].

Khorishko, L (2022) and Rudneva, A. & Malyovana, Yu. (2022) are convinced that the current military and political realities make it urgent for the Ukrainian leadership to seek additional resources to increase the state's capabilities in its activities in the international arena. In terms of Ukraine's information policy in the international format, the urgent task is to develop mechanisms to counter disinformation by the aggressor country on the basis of the fundamental constitutional principle of freedom of speech, taking into account the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and other international legal documents[37]. In view of this, according to Rudneva, A. & Malyovana, Yu. (2022), it is advisable to use public diplomacy tools, such as organising special events, setting the agenda, dialogue with the target audience, etc.[38].

Taking into account such opinions expressed by scholars, as well as trends in the cyberisation of the global information space, it is logical for Ukraine to use cyber diplomacy tools in its public diplomatic format to counter Russian information aggression. The political, legal and organisational conditions for this include, first of all, the existence of the concept of 'cyberspace' in Ukrainian legislation, which means 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[39].

The necessary legal framework is created by the Information Security Strategy (2021), Cybersecurity Strategy of Ukraine: Secure Cyberspace is the Key to Successful Development of the Country (2021) and Public Diplomacy Strategy of the Ministry of Foreign Affairs of Ukraine for 2021–2025 (2021). On this basis, in order to respond to the challenges of the digital age in a timely and high-quality manner in 2023. The Ministry of Foreign Affairs of Ukraine has started developing the Strategy of Cyber Diplomacy of Ukraine. A cyber diplomacy unit has been set up within the Ministry, the network infrastructure

[36] Данильян О.Г., Дзьобань О.П. Інформаційна війна у медіапросторі сучасного суспільства. Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія. 2022. № 3. С. 17–20.

[37] Хорішко Л.С. Публічна дипломатія України в умовах сучасної політичної дійсності. Політикус. 2022. № 3. С. 60–61.; Марущак А.І. Передумови для формування правових механізмів протидії дезінформації в соціальних медіа у контексті національної безпеки: постановка проблеми. *Інформація і право.* 2022. № 1(40). С. 85–87.

[38] Руднєва А., Мальована Ю. Інформаційний фронт російської агресії в Україні. Вісник Львівського університету. Серія філософсько-політологічні студії. 2022. № 45. С. 187–190.

[39] Закон України «Про основні засади забезпечення кібербезпеки України». Відомості Верховної Ради. 2017. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

is being actively developed, and training has begun, as well as a system of measures to digitalise the processes associated with the daily activities of the diplomatic service. The leaders of this ministry understand cyber diplomacy as 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, government policies on the development of the Internet, etc.[40]

Ensuring the information security of society is laid down in the Cybersecurity Strategy of Ukraine and the Information Security Doctrine. Both documents provide for the creation of all possible measures to ensure the safe functioning of cyberspace and counteract the information aggression of the Russian Federation. 'The Cybersecurity Strategy of Ukraine envisages the development of cyberspace protection, which is the basis for the protection of human rights. The priority areas of the documents include: 1) development of a safe and reliable cyberspace; 2) protection of state electronic information resources and information infrastructure; 3) protection of critical infrastructure; 4) development of the security and defence sector's capacity in the field of cybersecurity; 5) combating cybercrime (Decree of the President of Ukraine, 27 January 2016). The 'Doctrine of Information Security of Ukraine' provides for the protection of the vital interests of society and the state from the aggression of the Russian Federation in the information space, in particular, aimed at 'propaganda of war, national or religious hatred, change of the constitutional order by force or violation of the sovereignty and territorial integrity of Ukraine' (Decree of the President of Ukraine, 29 December 2016).

At the same time, the lack of critical perception of information by society, the lack of means to protect the information space, and sometimes the corruption component that allows pro-Russian media to conduct propaganda, are responsible for Ukraine's failures in the information war. The state should form its own powerful project that can reach the entire audience, subject to cooperation with other organisations. This way, society will see not only the refutation of false news, but also the official position of the state. To do this, it is necessary to create a strong legal framework that would regulate the

[40] У Львівському університеті розмовляли про цифрову дипломатію. URL: https://galinfo.com.ua/news/u_lvivskomu_universyteti_rozmovlyaly_pro_tsyfrovu_dyplomatiyu_409777.html; МЗС розробляє Стратегію кібердипломатії України – заступник міністра. 15.05.2024. URL: https://www.ukrinform.ua/rubric-polytics/3863944-mzs-rozroblae-strategiu-kiberdiplomatii-ukraini-zastupnik-ministra.html; Стратегія кібербезпеки України. Ббезпечний кіберпростір – запорука успішного розвитку України [Затверджено Указом Президента України від 26 серпня 2021 року №447/2021]. URL: https://www.president.gov.ua/documents/4472021-40013; Стратегія інформаційної безпеки: [Затверджено Указом Президента України від 28 грудня 2021 року № 685/2021]. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

security of the information space and, on the basis of scientific institutions or think tanks, organise a system of counter-propaganda and countering disinformation, while not forgetting basic democratic principles. At the same time, the state must stimulate the development of the IT sector, in particular in the security system, taking into account the latest challenges and foreign policy threats[41].

An important next step is 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 – cyber diplomacy. The lawmakers propose that cyber diplomacy 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, taking into account current needs[42].

Equally important in the context of the organisational and legal framework for the development of Ukraine's cyber diplomacy is the support provided by its allies. In particular, back in 2017, a bilateral cyber dialogue was launched between the United States and Ukraine, which provides a basis for further joint efforts to counter disinformation. Within its framework, the United States is making efforts to improve Ukraine's ability to respond to Russian disinformation and propaganda activities in cyberspace, including through social media and other media[43].

However, despite all this, it should be noted that today in the scientific field and media space of Ukraine there is no intensive discussion of the use of cyber diplomacy tools in countering Russian information aggression. As Barrinha, A. & Renard, T. (2017) point out, in order to neutralise the effects of information warfare, the victim of aggression must use the same technologies and methods of information warfare as the aggressor, but for its own purposes. Today, this primarily 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

[41] Вакулич В., Новородовська Н. Російська пропаганда агресії проти України (2014–2021 рр.). *Український інформаційний простір*. 2023. № 1. С. 126–128.

[42] Комітет розглянув законопроект про внесення змін до Закону України "Про дипломатичну службу" щодо вдосконалення проходження дипломатичної служби. 23 лютого 2024. URL: https://komsamovr.rada.gov.ua/print/84176.html; Україні пропонують кібердипломатію. 06 березня, 2024. URL: https://zn.ua/ukr/UKRAINE/ukrajini-proponujut-kiberdiplomatiju.html

[43] Марущак А. І. Передумови для формування правових механізмів протидії дезінформації в соціальних медіа у контексті національної безпеки: постановка проблеми. *Інформація і право.* 2022. № 1(40). С. 82–88.

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. In our opinion, the main reason for the impossibility of using the traditional tools of public diplomacy of the MFA institutionalised in Ukraine to address the challenges of countering Russian information aggression through cyber diplomacy 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. Supporting the above statements by Plohiy, S. (2022) and Pomerantsev, R. (2015) about the insufficiency of journalism resources in this regard, we believe it is appropriate to draw attention to the resources of public diplomacy as a type of public diplomacy and a tool of cyber diplomacy in its public diplomatic format[44].

Since the nineteenth century, the term 'public diplomacy' has been used to refer to open activities and specific official efforts aimed at influencing foreign public opinion in order to achieve diplomatic goals. The modern interpretation of this concept, which refers to a type of diplomatic activity, was laid down 60 years ago by American scholars J. Nye and E. Gullion. They defined public diplomacy as an instrument of soft power in international communications. By complementing classical diplomatic activities with new methods and including the societies of the countries that communicate with each other in diplomatic dialogue/political dialogue, public diplomacy promotes a positive image of the state based on the principles of human rights, tolerance, intercultural communication, which are necessary for overall sustainable institutional development and the search for ways to prevent and peacefully resolve conflicts and wars. In the last third of the twentieth and early twenty-first 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. At the same time, an important characteristic of public diplomacy is the way in which it communicates between the government and the public of other countries to form an understanding of national ideas, values, institutions, culture, national goals and policies, which involves actions in the field of information, education, and culture to influence foreign governments through the citizens of a particular country. An important task of such interaction is the need to influence, inform

[44] Сергій Плохій: «Ця війна є війною за всю Європу». URL: https://zbruc.eu/node/110984; Пітер Померанцев: «Мета російської пропаганди – щоб ніхто нікому не довіряв». URL: http://www.pravda.com.ua/articles/2015/03/31/7063251/

and activate the public to support national interests in the implementation of foreign policy.

The nature of public diplomacy has changed in the last half of the twentieth and early twenty-first centuries. The main reason for this is primarily the growing influence of the public and the intensification of interpersonal contacts. At the same time, an important characteristic of public diplomacy is the way in which it communicates between governments and the public of other countries to form an understanding of national ideas, values, institutions, culture, national goals and policies, which involves actions in the field of information, education, and culture to influence foreign governments through the citizens of a particular country. An important task of such interaction is the need to influence, inform and activate the public to support national interests in the implementation of foreign policy[45]. However, the qualitative shifts in public diplomacy are also due to the new realities of global social communications, which were influenced by the scientific and technological revolution and the emergence of new communication technologies that have formed a fundamentally new space of human existence – cyberspace.

American scholars, depending on the subject of public diplomacy activities, distinguish two main types of public diplomacy: 1) activities carried out by the state, under its leadership or at public expense within the framework of the state's foreign policy to implement the national interest – public diplomacy; 2) activities carried out by various individuals and legal entities, civil society institutions independently of the state in the interests of the state, society or the whole of humanity (citizen diplomacy). In both areas, the goal is to establish permanent contacts between civil society institutions in different countries, develop international networks and participate in their activities, while weakening state control and creating an atmosphere of trust and equality. In the United States, for example, according to the concept of citizen/civil diplomacy, every citizen has the right or even the duty to help the state implement its foreign policy. The subjects of such diplomacy can be students, teachers, scientists, athletes, business representatives, etc. – in this way, public interests are lobbied for. Sukhorolska, I. (2022) identifies the main five features of public diplomacy at the current stage of its evolution as openness and democracy; moving away from superficiality; increasing the role of values; turning into an equal game between different participants; dynamism and unpredictability. It is a complex interaction in a network of many different levels of actors, when civil society groups in different

[45] Кукалець О.Є. Публічна дипломатія в теорії міжнародних відносин. Наукові записки студентів та аспірантів. Серія «Міжнародні відносини». 2020. Вип. 5. С. 142–145.; Братута О., Братута Є. Публічна дипломатія: термінологічні, онтологічні та прикладні результати дослідження. Україна дипломатична. 2024. № 24. С. 737–738.

countries can act as initiators, active participants and partners of their states, as well as target audiences for programmes of foreign governments, corporations and organisations[46].

In addition, the Constitution of Ukraine (1996) in its Article 17 states that the protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic and information security are the most important functions of the state, the business of the entire Ukrainian people[47].

Based on these provisions, citizen/civil diplomacy can become a full-fledged tool of cyber diplomacy in countering Russia's information aggression against Ukraine. It seems that Ukrainian scientists, politicians, journalists, students and the public in general will contribute to the promotion of Ukrainian interests in the world by preparing and publishing content on media platforms and social networks that debunks fake, disinformation and propaganda narratives of an anti-Ukrainian nature and thus influence the positive image of the Ukrainian state. Of course, the language barrier may become 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 could be the organisation of multichannel media platforms (websites), which would host information materials of relevant content and educational content compiled by reputable scholars, politicians, and intellectuals, which would be available to foreign audiences in their languages. In general, the field for creative activity of the Ukrainian public in this regard is wide. It should also be emphasised that such activities will also strengthen the identity of communication participants on the part of Ukraine, as a person's perception of himself or herself as a member of a community that defends its information sovereignty and debunks false narratives about his or her country is a powerful factor of individual and collective self-identification.

CONCLUSIONS

In the digital age, the human lifestyle is changing qualitatively – life seems impossible without virtual reality and communications in cyberspace. In the mass communication aspect, there is a process of demassification that affects social relations in network communication. This is accompanied by information personalisation. Information aggression and information violence are becoming widespread. In cases where information influence determines a radical change in the addressee's train of thought, his or her perceptions of a particular phenomenon and levelling his or her assessments in the direction

[46] Сухорольська І., Климчук І. Громадська (публічна) дипломатія в умовах агресивної війни Росії проти України. Вісник Львівського університету. Філософсько-політологічні студії. 2022. № 43. С. 327–329.

[47] Конституція України [прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 року]. URL: https://www.president.gov.ua/documents/constitution

desired by the addressee with the use of coercive tactics through intimidation, then such mass information influence should be qualified as information terrorism.

Russia's hybrid aggression against Ukraine, which began in 2014 and included anti-Ukrainian information activities (propaganda, information manipulation, disinformation, fakes) as part of the entire complex of forceful actions, is fully consistent with the concepts of "information violence" and "information terrorism", since, in addition to hostile information influences of a destructive nature, it aims to change the identity of Ukrainians, to reconstruct and "recode" Ukrainian society as a whole. This is an information war against Ukraine, the most important task of which, in addition to manipulating the masses and introducing hostile, harmful ideas and views into the public and individual consciousness, is to destroy not the population, but the state mechanism. Everything Ukrainian – the government, state, society, culture and identity of Ukrainians, as well as the public perception of them in foreign countries – was targeted in order to undermine Ukraine's international authority, create a negative image of Ukraine and prevent large-scale military, economic and financial assistance to it by Western allies.

Cyber diplomacy, which includes a full range of diplomatic measures and is carried out in cyberspace, has become a response to such information challenges. At the same time, it has both a technological dimension and a purely public diplomatic one, associated with relevant social communications.

Since 2021, Ukraine has been creating the necessary legal framework to institutionalise its own cyber diplomacy. In 2023. the Ministry of Foreign Affairs of Ukraine started developing the Strategy of Cyber Diplomacy of UkraineAn important next step is to draft amendments to the Law of Ukraine "On the Diplomatic Service", which would give this service the authority to promote and protect national interests in cyberspace. Citizen/civil diplomacy, which also needs to be institutionalised, can become a full-fledged cyber diplomacy tool in countering Russia's information aggression. In general, the call of the times is to form a strong regulatory framework to regulate the security of the information space and to organise a system of counter-propaganda and countering disinformation, given the new challenges and foreign policy threats that Ukraine has faced in the last decade in the context of the need to counter Russia's total aggression.

SUMMARY

It is proved that qualitative changes in human life in the digital age in terms of mass communication are accompanied by the use of coercive tactics through intimidation and destructive mass information influences, which should be qualified as information violence and information terrorism. It is

emphasised that Russia's hybrid aggression against Ukraine, which includes anti-Ukrainian information activities (propaganda, information manipulation, disinformation, fakes) as a component of the entire complex of military actions, is an information war against Ukraine, the most important task of which is to destroy its state mechanism. It is substantiated that the answer to such information challenges is cyber diplomacy as a set of diplomatic measures carried out in cyberspace. It is concluded that in order to institutionalise its own cyber diplomacy, Ukraine needs to form a powerful legal framework for regulating the security of information space and countering Russia's total aggression.

References

1. Братута О., Братута Є. Публічна дипломатія: термінологічні, онтологічні та прикладні результати дослідження. *Україна дипломатична.* 2024. № 24. С. 727–740. doi: https://doi.org/10.37837/2707-7683-2023-40
2. Вакулич В., Новородовська Н. Російська пропаганда агресії проти України (2014–2021 рр.). *Український інформаційний простір*. 2023. № 1. С. 119–132.
3. Ващенко Н. Головні наративи сучасної російської пропаганди як впливогенна проблематика в умовах консцієнтальної війни Росії проти України. *Наукові записки інституту журналістики.* 2020. № 1(76). С. 180–201. doi: 10.17721/2522-1272.2020.76.15.
4. Верховцева І. Г. Російська інформаційна війна проти України 2014–2024 рр. як предмет наукових студій: концепт «інформаційне насильство». *Образ*. 2024. № 2(45). С. 26–35. DOI https://doi.org/10.21272/Obraz.2024.2(45)-26-35
5. Верховцева І.Г. Інформаційно-комунікаційний сегмент гібридної війни росії проти України 2014–2024 рр.: пропаганда (стан вітчизняних студій). *Наукові праці Національної бібліотеки України імені В. І. Вернадського*. 2024. Вип. 70. С. 443–477. DOI: 10.15407/np.70.443
6. Верховцева І.Г. Фейки російської інформаційної війни проти України: деконструюючи «руський мир» та «історичну росію». *Україна в умовах російської агресії: виклики та відповіді*: монографія / [І.В. Букрєєва, І.Г. Верховцева, В.В. Гулай та ін.]. Харків: Право, 2024. С. 76–93. Kharkiv: Pravo. DOI: https://doi.org/9786178518240
7. Висоцький О.Ю. Публічна дипломатія: конспект лекцій. Ч. І. Дніпро: СПД «Охотнік», 2020. 56 с.
8. Висоцький О. Iphone-дипломатія президента України в контексті новацій української цифрової дипломатії під час широкомасштабної російської агресії. *Україна і світ: теоретичні та*

практичні аспекти діяльності у сфері міжнародних відносин: матер. Міжнар. наук.-практ. конф., м. Київ, 11–12 квіт. 2024 р. Київ: Вид. центр КНУКіМ, 2024. С. 17–22.

9. Війни інформаційної епохи: міждисциплінарний дискурс: монографія / за ред. В. А. Кротюка. Харків: ФОП Федорко М. Ю., 2021. 558 с.

10. Данильян О. Г., Дзьобань О. П. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія.* 2022. № 3. С. 11–29. doi: 10.21564/2663-5704.54.265589

11. Дем'яненко М. Протидія інформаційній агресії: світовий досвід та вітчизняні реалії. *Наукові праці Національної бібліотеки України імені В. І. Вернадського.* 2018. № 50. С. 225–240.

12. Дзеркаль В. Інструменти кібер-дипломатії у реалізації зовнішньої політики держави. *Актуальні проблеми сучасних міжнародних відносин.* Матеріали Всеукраїнської науково-практичної конференції. 17-18 листопада 2023 р., м. Дніпро. / ред. кол.: І.В. Іщенко, І.К. Головко, П.Г. Петров. Дніпро: ПрінтДім, 2023. С. 198–200.

13. Жайворонок О.І. Міжнародний досвід протидії інформаційному тероризму та його імплементація в Україні. *Публічне управління та митне адміністрування*. 2020. № 1(24). С. 91–96.

14. Закон України «Про основні засади забезпечення кібербезпеки України». *Відомості Верховної Ради.* 2017. № 45. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

15. Іщук Н. М. Демасифікація як соціальна трансформація: прогнози та реалії. *Актуальні питання масової комунікації.* К., 2013. Вип. 14. С. 14–19.

16. Іщук Н. М. Персоналізація інформації в мережевій комунікації: переваги та недоліки. *Наукові записки Інституту журналістики*. К., 2015. Т. 58. С. 134–139.

17. Комар О. Soft power і пропаганда у російсько-українській війні: епістемологічний аналіз. *Українознавчий альманах*. 2022. № 30. С. 82–88. doi: 10.17721/2520-2626/2022.30.11

18. Конституція України [прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року]. URL: https://www.president.gov.ua/documents/constitution

19. Кукалець О.Є. Публічна дипломатія в теорії міжнародних відносин. *Наукові записки студентів та аспірантів. Серія «Міжнародні відносини».* 2020. Вип. 5. С. 141–147.

20. Курбан О.В. Сучасні інформаційні війни в мережевому он-лайн просторі. Київ: ВІКНУ, 2016. 286 с.

21. Марущак А.І. Передумови для формування правових механізмів протидії дезінформації в соціальних медіа у контексті національної безпеки: постановка проблеми. *Інформація і право.* 2022. № 1(40). С. 82–88.

22. Матвієнко В., Петушкова Г. Кібердипломатія в Європейському Союзі: модель естонської кібердипломатії та досвід України. *Україна дипломатична.* 2024. Вип. XXIV. С. 696–708.

23. Мельник Д.С., Леонов Б.Д. Інформаційний тероризм як загроза національній інформаційній інфраструктурі. *Інформація і право.* 2024. № 3(50). С. 99–107.

24. Мельніченко О.А. Основні напрями деструктивної діяльності російських спецслужб в інформаційній війні проти України. *Гібридна війна: сутність, виклики та загрози*: збірн. матер. круглого столу (Київ, 8 липня 2021 р.). Київ: НА СБУ, 2021. С. 31–38.

25. МЗС розробляє Стратегію кібердипломатії України – заступник міністра. 15.05.2024. URL: https://www.ukrinform.ua/rubric-polytics/3863944-mzs-rozroblae-strategiu-kiberdiplomatii-ukraini-zastupnik-ministra.html

26. Нарис теорії і практики інформаційно-психологічних операцій / Дзюба М.Т., Жарков Я.М., Ольховой І.О., Онищук М.І. Київ: ВІТІ НТУУ "КПІ", 2006. 471 с.

27. Пасічна В. Кібердипломатія та її вплив на інформаційне суспільство. *Цифрова дипломатія України: синергія реального і віртуального.* Матеріали міжнародної наукової конференції. Львів, 24 листопада 2023 р. / Упорядники: М. Мальський, Р. Вовк, О. Кучик. Львів: ЛНУ імені Івана Франка, 2023. С. 79–81.

28. Пітер Померанцев: «Мета російської пропаганди – щоб ніхто нікому не довіряв». URL: http://www.pravda.com.ua/articles/2015/03/31/7063251/

29. Почепцов Г. Смислові та інформаційні війни. *Інформаційне суспільство*. 2013. Вип. 18. С. 21–27.

30. Проноза І.І. Інформаційна війна: сутність та особливості прояву. *Актуальні проблеми політики*: збірн. наук. праць. 2018. Вип. 61. С. 76–84.

31. Радчич С. Философское осмысление феномена современной информационной войны. URL: https://www.academia.edu/82161813/%D0%A4%D0%B8%D0%BB%D0%BE%D1%81%D0%BE%D1%84%D1%81%D0%BA%D0%BE%D0%B5_%D0%BE%D1%81%D0%BC%D1%8B%D1%81%D0%BB%D0%B5%D0%BD%D0%B8%D0%B5_%D1%84%D0%B5%D0%BD%D0%BE%D0%BC%D0%B5%D0%BD%D0%B0_%D1%81%D0%BE%D0%B2%D1%80%D0%B5%D0%BC%D0%B5%D0%BD%D0%BD%D0%BE%D0%B9_%D0

%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9_%D0%B2%D0%BE%D0%B9%D0%BD%D1%8B

32. Руднєва А., Мальована Ю. Інформаційний фронт російської агресії в Україні. *Вісник Львівського університету. Серія філософсько-політологічні студії.* 2022. № 45. С. 186–192.

33. Рульов І. Співвідношення кібертероризму та кіберзлочину. *Юридичний вісник.* 2021. № 3. С. 178–185.

34. Росія поширює в Ізраїлі фейки про Україну на «популярних сайтах». URL: https://www.ukrinform.ua/rubric-world/3738744-rosia-posirue-v-izraili-fejki-pro-ukrainu-na-popularnih-sajtah-zmi.html

35. Савич А.С. Комунікативні інструменти протидії інформаційної агресії Росії: світовий досвід. *Вісник Маріупольського державного університету. Серія: Історія. Політологія.* 2015. Вип. 12. С. 270–277.

36. Сергій Плохій: «Ця війна є війною за всю Європу». URL: https://zbruc.eu/node/110984

37. Смачило Т.В., Кривцун А.Р. Феномен інформаційного тероризму як загрози міжнародній безпеці. *Молодий вчений.* 2017. № 11. С. 124–127.

38. Стратегія інформаційної безпеки: [Затверджено Указом Президента України від 28 грудня 2021 року № 685/2021]. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text

39. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку України [Затверджено Указом Президента України від 26 серпня 2021 року № 447/2021]. URL: https://www.president.gov.ua/documents/4472021-40013

40. Сухорольська І., Климчук І. Громадська (публічна) дипломатія в умовах агресивної війни Росії проти України. *Вісник Львівського університету. Філософсько-політологічні студії.* 2022. № 43. С. 322–331.

41. Комітет розглянув законопроект про внесення змін до Закону України "Про дипломатичну службу" щодо вдосконалення проходження дипломатичної служби. 23 лютого 2024. URL: https://komsamovr.rada.gov.ua/print/84176.html

42. Требін М.П. Цифрове суспільство: спроба проникнення в сутність. *Цифрова епоха: міждисциплінарний дискурс*: монографія. Харків: Право, 2024. С. 4–30.

43. Требін М.П. Цифровізація як мегатренд сучасного бутя. *Цифрова епоха: міждисциплінарний дискурс*: монографія. Харків: Право, 2024. С. 31–55.

44. Требін М.П. Феномен інформаційної війни у світі, що глобалізується. *Вісник Національного університету "Юридична*

академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія. 2013. № 2. С. 188–198.

45. У Львівському університеті розмовляли про цифрову дипломатію. URL: https://galinfo.com.ua/news/u_lvivskomu_universyteti_rozmovlyaly_pro_tsyfrovu_dyplomatiyu_409777.html

46. Удавана Росія: імітація величі і могутності / Зеленько Г. (кер. проєкту, наук. редактор) та ін. Ніжин: Вид. Лисенко М.М., 2024. 288 с.

47. Україні пропонують кібердипломатію. 06 березня, 2024. URL: https://zn.ua/ukr/UKRAINE/ukrajini-proponujut-kiberdiplomatiju.html

48. Харитоненко О.І., Харчук О.В. Визначення, види, актуальні напрямки дослідження інформаційних війн. *Гібридна війна і журналістика проблеми інформаційної безпеки* / за заг. ред. В. О. Жадька. К.: Вид-во НПУ імені М.П. Драгоманова, 2018. С. 32–63.

49. Хорішко Л.С. Публічна дипломатія України в умовах сучасної політичної дійсності. *Політикус.* 2022. № 3. С. 60–64. doi: https://doi.org/10.24195/2414– 9616.2022-3.9

50. Al-Muftah, H., Weerakkody, V., Rana, N.P., Sivarajah, U., & Irani, Z. (2018). Factors 200 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

51. Barrinha A., Renard T. (2017). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs*, 3(4-5), 353–364.

52. Christou, G. (2024). Cyber Diplomacy: From Concept to Practice. *Tallinn Paper, 14.* URL: https://ccdcoe.org/uploads/2024/06/Tallinn_Papers_Cyber_Diplomacy_From_Concept_to_Practice_Christou.pdf

53. *Deputy Secretary General Opens First International Conference on Cyber Diplomacy, Building Global Digitalization* (2022). Retrieved from https://www.nato.int/cps/en/natohq/news_195445.htm

54. Dorschner, J. (2015). Hybrid War in the Near Abroad. *IHS: Jane's Defence Weekly, 52-10,* 24–30.

55. 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

56. Libicki, M. (2009). *What is Information Warfare, National Defense University*. Retrieved from http://www.iwar.org.uk/iwar/resources/ndu/infowar/a003cont.html

57. Petkun S., Verkhovtseva I. Hostile Propaganda Of The Digital Age As Information Violence: Ukraine's Response To Russian Information Invasion. *Modern Science: Prospects, Innovations And Technologies*: Scientific Monograph. Part 1. Ryga: Izdevnieciba "Baltija Publishing", 2024. P. 445–485. DOI: https://doi.org/10.30525/978-9934-26-473-3-16

58. Pocheptsov, G. Russian Propaganda Wars: Russia – Ukraine 2022. URL: https://www.academia.edu/95759898/Pocheptsov_G_Russian_propaganda_wars_Russia_Ukraine_2022_https_www_kvak_ee_files_2023_01_Sojateadlane_20_2022_Georgy_Pocheptsov_RUSSIAN_PROPAGANDA_WARS_RUSSIA_UKRAINE_2022_pdf?email_work_card=title

59. Rácz, A. (2015). *Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist.* Helsinki: Ulkopoliittinen Instituutti Utrikespolitiska Institutet; The Finnish Institute Of International Affairs.

60. Robinson, R. Cyber Diplomacy: A New Frontier in International Relations and Professional Practice. *EDRM.* Retrieved from https://edrm.net/2024/06/cyber-diplomacy-a-new-frontier-in-international-relations-and-professional-practice/

61. What is cyber diplomacy? Retrieved from https://www.cyber-diplomacy-toolbox.com/Cyber_Diplomacy.html

Information about the authors:
Petkun Svitlana Mykhailivna,
Doctor of Public administration, Associate Professor,
Head of the Department of Public Administration and Managemen
State University of Information and Communication Technologies
7, Solomianska St., Kyiv, 03100, Ukraine

Verkhovtseva Iryna Gennadiivna,
Doctor of History, Associate Professor,
Professor of Department of Public Administration and Management
State University of Information and Communication Technologies
7, Solomianska St., Kyiv, 03100, Ukraine