DOI: https://doi.org/10.34069/AI/2021.45.09.3

How to Cite:
Sheremet, O. S., Voluiko, O. M., Posmitna, V. V., Poda, T., & Bidzilya, Y. M. (2021). Political and legal aspects of the information warfare. Amazonia Investiga, 10(45), 31-41. https://doi.org/10.34069/AI/2021.45.09.3

Political and legal aspects of the information warfare

Політико-правові аспекти інформаційної війни

Received: July 20, 2021 Accepted: September 15, 2021

Written by:
Oleg S. Sheremet[7]
https://orcid.org/0000-0002-9512-991X
Oleksii M. Voluiko[8]
https://orcid.org/0000-0002-0894-5004
Victoriia V. Posmitna[9]
https://orcid.org/0000-0001-8719-1767
Tetiana Poda[10]
https://orcid.org/0000-0001-9662-1204
Yuriy M. Bidzilya[11]
https://orcid.org/0000-0001-5134-3239

Abstract

This article describes the technological features of information warfare and possible lawful mechanisms to counter information attacks. The aim of the article is to analyse the political and legal features of information warfare. The tactics of the aggressor state's behaviour in a hybrid war was substantiated using the case of the information war between Russia and Ukraine. The channels of information dissemination, which are most often used for disintegration and disinformation purposes, were studied. Problematic issues of the domestic public space that most often appear in the perspective of disinformation attacks on the Internet are determined: the activities of the Armed Forces of Ukraine, cooperation between Ukraine and the EU, reforms in Ukrainian society, temporarily occupied territories and annexed Crimea, corruption in Ukraine. The tactics of confrontation between countries in the information space was analysed — attempts to establish their "security belt" from other actors in international relations and to maintain their own

Анотація

У цій статті описано технологічні особливості інформаційної війни та можливі законні механізми протидії інформаційним атакам. Метою статті є аналіз політико-правових особливостей інформаційної війни. Тактика поведінки держави-агресора в гібридній війні була обґрунтована на прикладі інформаційної війни між Росією та Україною. Вивчено канали розповсюдження інформації, які найчастіше використовуються для дезінтеграції та дезінформації. Визначаються проблемні питання вітчизняного публічного простору, які найчастіше виникають у перспективі дезінформаційних атак в Інтернеті: діяльність Збройних Сил України, співпраця між Україною та ЄС, реформи у Українське суспільство, тимчасово окуповані території та анексований Крим, корупція в Україні. Проаналізовано тактику протистояння між країнами в інформаційному просторі - спроби встановити свій "пояс безпеки" від інших суб'єктів міжнародних відносин та зберегти

[7] Doctor of Law, Associate Professor of the Department of Law, Philosophy and Political Science of O.M. Lazarevskyi Institute of History and Socio-humanitarian Disciplines of Taras Shevchenko National University "Chernihiv Collegium", Ukraine.
[8] PhD in Juridical Sciences, Head of the Department of Legal Support of Military-combat Activity of the Kyiv Faculty of the National Academy of the National Guard of Ukraine, Ukraine.
[9] PhD in Philological Science, Associate Professor of the Department of Legal Support of Military-combat Activity of the Kyiv Faculty of the National Academy of the National Guard of Ukraine, Ukraine.
[10] PhD in Philosophy, Associate Professor of the Department of Philosophy, Faculty of Linguistics and Social Communications, National Aviation University, Ukraine.
[11] Doctor of Social Communications, Professor, Head of the Department of Journalism, Faculty of Philology, Uzhhorod National University, Ukraine.

dominant influence in certain regions by spreading misinformation. Promising areas of further research will be the analysis of the peculiarities of the national legal systems' development in order to counter misinformation in the context of the continuous development of democracy in the world.

Keywords: Information war, misinformation, political and legal aspects, mental aggression, media development, mass media, social networks.

власний домінуючий вплив у певних регіонах шляхом поширення дезінформації. Перспективними напрямами подальших досліджень буде аналіз особливостей розвитку національних правових систем з метою протидії дезінформації в контексті постійного розвитку демократії у світі.

Ключові слова: Інформаційна війна, дезінформація, політичні та правові аспекти, психічна агресія, розвиток ЗМІ, ЗМІ, соціальні мережі.

Introduction

Information war is the most common form of modern confrontation, targeting human consciousness (Easton & Almond, 2016; Batyuk, 2017). It is based on the ability to control and manipulate public opinion, that is playing up to the human will. People live in the information space and receive information from the Internet, press, radio and television programmes on a daily basis. In a symbolic world that is separate from reality, they may even conflict with their own interests. Reality has receded into the background. People are not free in this sense, especially because there are many ways to effectively influence information. There is the term "brainwashing", which can create a passive, flexible person and turn his/her into a controlled group. Overcoming the threats posed by information wars is a factor in national security. Information wars lead to the destruction of the unified information space of the state, manipulation of public consciousness, illegal use of special means of influencing public consciousness, as well as intensification of international competition for the possession of information technology and resources.

One of the factors contributing to the emergence of information wars is the inadequate regulation of relations in the information sphere, as well as insufficient practice of law enforcement in disinformation processes. This determines the topicality of this research. The formation of public consciousness with the help of the subjects of information war using the methods of psychological influence is becoming the most effective way of control and manipulation both within the state and abroad. It all depends on who actually determines the information content.

Russia's political and information war against Ukraine has become a long-term factor affecting the country's national security. It is necessary to develop an effective concept of information security to combat this impact.

Therefore, the aim of this work is to explore the political and legal aspects of information warfare and the mythologising of public consciousness that accompanies this process. This aim involves fulfilment of the following research objectives: 1) analysis of the features of information wars, misinformation and mediatisation of political consciousness to ensure the goals of individual policy actors; 2) identification of problems of active involvement of states in the processes of counteracting threats in the information space.

Literature review

There are three main goals in the information war: control over the information space and ensuring the protection of one's information from hostile actions; use of control over the information space for information attacks on the enemy; increasing the overall efficiency of information functions. According to a number of theorists, continuing to stop broadcasting pro-Russian TV and radio channels and disseminating anti-Ukrainian information, quickly refuting false information about Russia in the Ukrainian media, reporting on government agencies in the most transparent way and improving media literacy of the Ukrainian people are effective means of levelling threats to Ukraine (Saakov, 2018; Bennett & Iyengar, 2010).

According to modern theorists, one of Russia's main tasks in the political, legal and information war against Ukraine are the following (Blank, 2016; Dodonov, 2015):

- creating an atmosphere with a negative attitude to the cultural and historical heritage of Ukrainian society;
- manipulation of public opinion and political orientation of the Ukrainian people to create political tension and chaotic country;

- destabilization of political relations between political parties, associations and movements in order to incite conflicts, arouse distrust, suspicion, aggravate hostility and struggle for power;
- discrediting the behaviour of top public servants of Ukraine;
- initiation of protests and disobedience;
- undermining the country's international prestige and cooperation with other countries;
- creation or strengthening opposition organisations or movements, especially the extreme right or the extreme left;
- discrediting the national history and national identity of Ukrainians;
- initiation of changes in worldviews and value systems;
- minimisation of information on achievements recognised in science, technology and other fields, focusing on shortcomings, consequences of wrong actions and unqualified government decisions;
- undermining the morale of the population (fatigue from war, political scandals, disbelief in victory) and, as a consequence, the reduction of defence capabilities and combat potential of the army;
- damage to critical infrastructure (hardware, software, protection tools and protection regime against unauthorised leakage).

Other theorists include the formation of preconditions for economic, mental or military disruption, loss of readiness to fight and win, destructive information-psychological, information-technical and ideological influence (Bukkvoll, 2016; Cassiday & Johnson, 2016).

The field of information warfare promotes the free flow of information. All actions in information conflicts are necessary to achieve the intended political priorities over the enemy. Information warfare implies the following actions: gaining social control, manipulating information, disinformation, propaganda (Bielawski & Radomska, 2017). Such influences can lead to political results, to a change in the political views of the enemy in an information war.

Regime change as an operational policy is supported by the control of selective information to create a comfortable perception of events and create a sense of legitimacy. The modern approach to political regime change and information warfare is to unleash an all-out attack through the information sphere (dissemination of selective information), thereby preventing politicians from adequately responding to the impending threat (Simons, 2021). Information systems are used by actors who want to undermine state institutions and political systems and create political upheavals by compromising public information systems (Desouza et al., 2019).

Between 2018 and 2021, the EU recorded more than 11,000 cases of misinformation, most of which concerned Ukraine. According to the representative of the European Commission, the spread of false information is increasing, which is a threat to democracy and damages the reputation of the media. Therefore, appropriate mechanisms should be developed to detect false information. We can say that a full-scale war is being waged against Ukraine: the form is "political" and the content is "asymmetric".

Thus, it is necessary to create special legislation aimed at legal support of information security, and the effective application of existing legislation, the rules of which often make it possible to effectively guarantee information security (Kharytonov et al., 2019). Given that information wars can lead to global threats and security, the need to develop a convention in accordance with international law to regulate the arena of information warfare becomes an urgent issue (Qureshi, 2019).

It is worth noting that according to the classical approach expressed in the book of the ancient Chinese strategist Sun Tzu — The Art of War — the nature of any war is deceptive. Therefore, most citizens of the country who have been attacked by political information are usually disoriented by large volumes of contradictory information, and do not understand the immediate scale and dangers for the whole country.

The Internet has become a disseminator of false information. The more people depend on social networking sites, the more likely they are to unknowingly come across information that could change their point of view and influence political behavior (Asri & Sualman, 2019). But it should be noted that other (traditional) media have also been involved in spreading misleading information about a certain population in certain countries and defending certain actions. First, they are not very effective, and electronic media can report fake news today. Second, publications in print media are documents, so both the author and the publication can be prosecuted. Due to its nature, radio is not suitable for disseminating

such information. Nowadays, television has gained unprecedented power, but there are two reasons why forgery may occur: negligence, unconfirmed information, incompetence of reporters and the decisive influence of the government on the national information policy of electronic media (Snegovaya, 2018; Gerbner, 2018).

For example, in Ukraine there are many publications that actively disseminate information of dubious quality, sometimes misinformation. For example, publications such as the false statement by Supreme Allied Commander Europe (NATO), General Breedlove about air strikes against Russian troops in Ukraine (published on the National Anti-Corruption Portal page) (Calha, 2015; Galeotti, 2017; Kurian, 2011). However, the number of fake news from Russian TV channels and Internet sources is very large. With the help of the Russian media, Vladimir Putin's regime has launched a real political war against Ukraine. Political war usually targets young people. Therefore, the emphasis on the spread of fake messages is concentrated in social networks, which are very popular among young people. To this end, the Russian authorities have set up the so-called "Internet troll factory" in St. Petersburg — young people who pretend to be real members of the Internet, widely concentrating and disseminating provocative and outrageous information. The purpose of this action is psychological treatment of citizens of Ukraine and other countries, including Internet users in Russia. The principle of operation of the "Troll Factory" is that "repeated lies become a fact", when users do not want to follow alternative opinions on any issues. An example of this activity is false information about the demolition of a giant Mother Homeland Monument on Pechersk Hill in Kyiv.

Methods and materials

Research design

The research procedure involved 2 stages:

1. The preparatory stage included content analysis of scientific literature on the selected topic, review of news headlines of the largest news media, secondary analysis of empirical data from analytical reports of international organisations.
2. The field stage involved conducting qualitative sociological research in the form of focus groups.

Methods

Well-known methods were used at the preparatory stage. Methods of qualitative data processing were used, which include statistical data of information sources on false media data, classification of methods. Theoretical research method allowed identifying the political and legal characteristics of information war. To strengthen it, empirical methods of scientific research were used: observations and generalisations, which involved obtaining facts about the information war, forecasting trends in the intervention of some states in the affairs of other states.

Qualitative methods of focus group interviews were used. This approach allowed getting a wide range of opinions and creating group dynamics to update and problematise issues related to countering information threats from different target groups.

Sample

Transcripts of 2 focus groups were obtained in the course of the field stage. A total of 2 focus group interviews were conducted: 1) with media representatives (8 respondents); 2) with representatives of public organisations and active citizens (8 respondents).

Both meetings took place online because of a pandemic. The study also used the method of secondary analysis of sociological data. Sociological surveys were used, which claim to be determined as mass and national. The sampling method was used in the process. The sample population was representative of the whole of Ukraine. The stratification principle was applied when building the sample. The strata were the regions of Ukraine, there are respondents from all regions of Ukraine. Confidence probability (accuracy) — 95%, error 2-3%.

A secondary analysis of the results of sociological survey was used to substantiate the functional threats of disorientation policy. In the course of the research, mass sociological surveys (Social Communications Research Center, Socis (https://socis.kiev.ua/ua), etc.) were analysed with a representative sample by gender, age, and territorial attributes. The general population in such studies averaged more than 2,000 people, with an error of no more than 2.5%.

Thus, the methodology of analysis of the subject of research is used, aimed at reflecting the

pluralistic positions of two important stakeholders, participants in the political and legal process. The behavioural approach, which connects the active position of the media and civil society in the context of information confrontations, has proved fruitful for the analysis of procedural aspects of information warfare.

Results and discussion

A cross-cutting line among the factors of the information war was the problem of insufficiently high abilities of citizens to think critically. Political, informational, media literacy is an important factor in counteracting real and potential information attacks (see Table 1).

Table 1.
Aspects of improving political and information literacy.

Item No.	Aspects	Description
1.	Verification	To maintain trust in the official or recognised media, Internet users need to take precautionary measures to avoid falling victim to misinformation. It is necessary to check any content received online, especially if you are going to use it and distribute it further. Verification technologies based on the help of volunteer users are becoming increasingly popular. Communities such as Bellingcat and #DigitalSherlocks, Stopfake view the verification and geolocation of volunteers as important team activities.
2.	Exposure	One of the problems that users need to consider is "inflation" of false stories — whether the misinformation is spreading further and even more as a result of the exposure of facts and publication of results, whether it does not give them too much publicity.
3.	Checking for correspondence to reality	Analyse the articles of journalists who study suspicious statements and verify the facts, answering questions from the audience.
4.	Media literacy	One of the best ways to stop the spread of misinformation is to spread information which helps the audience to critically evaluate the information they read on social networks.

Source: compiled by the authors

An example of resistance in the information confrontation was the new project Information as a Weapon. Materials for the development of media literacy are published daily on the official website of the organization Svoboda. These materials reveal the essence of information war, principles of behaviour, tasks, classification of information weapons, features and methods of its use. Ukraine's Strategic Plan brings together politicians, experts, analysts, journalists and public figures to improve Ukraine's national security. The purpose of its activities is to participate in the formation and decision-making on national security issues to improve Ukraine's defence capabilities, reform the national security and defence sector in accordance with NATO standards, promote Ukraine's integration into the Euro-Atlantic security framework.

At the same time, in countries with totalitarian political regimes, television is the main focus of the most powerful, impressive, accessible and widely used media (Table 2).

Table 2.
Political and informational trust of citizens in the media.

Item No.	Type of information resource	Ration in %
1.	Television	82%
2.	Web-site news	55%
3.	Social networks	52%
4.	Radio	28%
5.	Print media	23%
6.	Television news	30%

Source: compiled by the authors

The television, which will rank first for a long time, was preferred by 82% of respondents (Zozulia, 2020). In the course of the research, we asked the same question in two focus groups — with representatives of the media and representatives of civil society institutions, active citizens — "What should be the actions of citizens in the information war"? We received the same answers in both focus groups: check information, reveal false stories, continuously improve information literacy.

During the focus groups (see Table 3), media representatives and active citizens strongly argued that national information security should now become a fundamental component of the national security strategy.

Table 3.
Generalised results of the focus groups conducted by the author (survey of media and civil society representatives on the topic of information war)

Question	Focus group with representatives of civil society institutions	Focus group with media representatives
In your opinion, what is the role of the state in counteracting misinformation?	Determinant — the state is responsible for the safety of citizens, including in the information sphere	The state's role is important, but it can weaken without the efforts of the public sector and an active position in the application of critical thinking by citizens
In your opinion, what is the participation of the media in counteracting information attacks?	Today's media does not always provide a fair and objective coverage of events. Therefore, their participation may entirely support information attacks or resist them	Determinant — the media with maximum responsibility are involved in the process of countering information attacks
In your opinion, what is the significance of the participatory role of civil society in counteracting information wars?	Civil society must be active and not indifferent to national security issues. But the state carries the main load in counteracting information threats. Citizens pay taxes, the state guarantees "information well-being"	Determinant — citizens set the pitch to the entire public discourse. The presence or absence of "information noise" in public discourse largely depends on their choice of which media to prefer, which topic to cover in this media, or to share certain information on social networks.

Source: compiled by the authors

Given the rapid development of information technology and the growing influence of the media, social networks, and other Internet monitoring resources, news agencies are used as the most common means of information warfare (information aggression).

International legal acts on information security provide for restrictions on freedom of speech to protect the rights and reputation of other person and/or to protect national security and public order, health and morals. On May 16, 2011, the UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, Hoffman (2014), submitted a report to the UN Human Rights Council on the main trends and problems of people in finding and transmitting information and ideas via the Internet.

This report also sets out general methods for restricting access to the Internet: 1) the law should provide for clear restrictions; 2) restrictions should be applied only to protect the rights and reputation of other persons and/or to protect national security and public order, health and morals (Article 19, paragraph 3, of the International Covenant on Civil and Political Rights); 3) the need to restrict freedom of speech must be proven. The application of the provisions requires prior confirmation of the facts of information aggression of one state against another, which can result in armed conflict, terrorist acts, sabotage, thousands of wounded, increased internal migration, number of refugees, and so on.

Given the urgent need to protect the national information space, the Parliament of Ukraine adopted, revised and amended some regulations. Thus, Article 5 of the Law of Ukraine "On Ensuring Civil Rights and Freedoms, and the Legal Regime on the Temporarily Occupied Territory of Ukraine" recognizes the Russian Federation as the occupying power. It should be noted that although there is much evidence that Ukraine still does not recognize Russia as an aggressor, there is reason to talk about a hybrid

nature of the confrontation (part of which is a targeted misinformation campaign) (Law No. 1207-VII, 2014).

Laws and draft laws on the establishment of a system for the protection of the national information space complement national legislation. In particular, it is the Decree of the President of Ukraine on approval of the decision of the National Security and Defence Council of Ukraine "On National Cybersecurity Threats and Emergency Measures to Eliminate Threats" and "On the Doctrine of Information Security of Ukraine" (February 2017) (Decree of the President of Ukraine № 47/2017, 2017); "On the Application of Personal Special Economic and Other Restrictive Measures (Sanctions)" (April 2017) (Decree of the President of Ukraine №133/2017, 2017); "On the Threat to National Cyber Security and Emergency Measures to Eliminate these Threats" (August 2017), the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (October 2017) (Law No. 2163-VIII, 2017).

These provisions have provoked a negative reaction of not only the media, but also practitioners and scholars in the legal field and other areas related to the provision of information. International Security Experts Pazyuk and Mitsik (2019) conducted a detailed legal analysis of the Decree of the President of Ukraine based on the decision of the National Security and Defence Council "On the Implementation of Certain Special Economic Measures and Other Restrictive Measures (Sanctions)". Experts concluded that some of the above provisions and other provisions of information laws and regulations do not take into account the technical components of the country's information security system. This directly affects the level of effectiveness of measures to ensure the national information field security, their implementation and management. The complexity of this situation increases the urgency of developing the legal aspects of modern information wars.

The actual situation of legal liability for violation of freedom of speech always has certain socio-economic consequences. Therefore, the Presidential Decree "On the Application of Personal Special Economic and Other Restrictive Measures (Sanctions)", which prohibits Internet service providers from providing resources to Internet users, does not comply with the principles of legality and legal grounds of such restriction. From a legal point of view, blocking Russian Internet resources is also a somewhat controversial step. Joining the "club" of countries that block Internet resources (Russia, North Korea and China) is a very controversial decision.

Prohibition is always the simplest and most unpleasant choice. This is not the right strategy for a country that seeks to implement European integration intentions. The view of the international community on this issue is undoubtedly negative. Blocking information resources can help rather than hinder propaganda. As a rule, it is difficult to provide a good confrontation without falling to the aggressor's level. In order to protect their democratic values, centuries-old traditions and achievements in the field of human rights, European countries are forced to find ways to restrict freedom of speech in order to protect this type of democracy. In fact, the effects of information aggression far outweigh the capabilities of conventional means, and it encourages temporary restrictions on democracy in order to uphold democratic values in the future. According to the focus groups, the opinion of representatives and active citizens was divided by about 50% to 50%: one half of the respondents were in favour of blocking Russian information resources in Ukraine, the other half were strongly against such radical steps at the state level.

Usually, measures in the field of information security include: formulation and implementation of information security strategy of Ukraine; introduction of a public register of owners/managers of Internet resources; creation of special state institutions to respond to information aggression; implementation of educational programmes of media literacy; creating favourable conditions for the promotion, development and accessibility of domestic book publishing, television and film production, education and culture; forced use of antivirus software; strengthening responsibility for the use of unlicensed software.

Analysis of the experience of the United States and European countries on legislation and regulations on information war shows that the main tools to combat the information disorientation campaign are the following: 1) the development of social information culture; 2) development of social information culture, introduction of specialised state and interstate institutions to combat and prevent cyberattacks; 3) creation of cyberpolice; 4) introduction of state registrars of Internet resources for dissemination of unreliable information

(misinformation, hostile propaganda, etc.); 5) development of national media education programmes; 6) introduction of economic sanctions on relevant entities in the information market; 7) a ban on the use of simulation tools and other information technology tools designed to manipulate public awareness in elections; 8) the obligation to disclose sources of funds for political advertising/advocacy in the media and social networks; 9) creation of software based on artificial intelligence technology for detection, identification and marking of false information; 10) creation of databases of information resources, analytical centers, tools for verifying information and messages, etc.

There were 90% of the respondents in the focus groups of media representatives and civil society institutions who agreed with the urgency and importance of such a step to ensure that information challenges in modern Ukraine are addressed within the legal field. The need to adopt the Information Code of Ukraine should be noted. This idea is enshrined in the Basic Principles for the Development of Information-Oriented Society in Ukraine for 2007-2015 (Zozulia, 2020; Stadnyk, 2017).

The study found that 90% of journalists and civic activists surveyed in the focus group considered the issue of consistent legal regulation to ensure the country's information security to be No. 1 problem. For a democracy, it is the most important tool for countering disinformation attacks by other countries. However, civil society is showing a tendency towards a somewhat paternalistic position of the state in ensuring information security. Media representatives have demonstrated a more proactive stance on their own responsibility to counter misinformation campaigns.

These views of the respondents are fully summarised with the positions of modern theorists. According to Barabash and Kotelenets (2016), the ability to influence public communication channels currently has a decisive impact on the level of legitimacy of government.

Kalpokas (2017) extends this opinion. In his works, he analyses the phenomenon of Internet branding and its importance in increasing threats to national security and political instability. According to the author, the state, which is considered as a brand, should project its image to both domestic and foreign audiences. However, when building a brand, states are vulnerable to "sofa warriors" — ordinary people who are involuntarily "recruited" by hostile actors to spread (through social media or other platforms) a counter-brand that is harmful to the state.

According to Akimenko, and Giles (2020), with the growing level of digitalisation in the modern world, the challenges of information wars will become more pronounced, political elites will identify them in the list of the most pressing threats to national unity.

Bilan (2016) considers it necessary to introduce Ukrainian information law. Today, the issue of improving Ukrainian information legislation in the creation, dissemination and use of information is very important in accordance with modern needs and challenges. According to domestic lawyers, this improvement should be done through codification, formulation and adoption of the Information Code of Ukraine. In particular, the famous Ukrainian scientist and politician Gorbulin supports this idea. This code would be especially important for the regulation of socio-political processes both for the population suffering from information confrontation and for the regulation of the state's position in the international community (Zozulia, 2020; Karber, 2015). In the case of Ukraine, we are dealing not only with hostile propaganda, but also with a "semantic (value-based, meaningful) war" correctly described by intelligence experts. The whole set of information communication is used to retransmit these values. The main structural element of this war is imitation images, which do not really exist. Examples of such imitations are "fascists in Kyiv", "cruelty of punitive forces", "punished guys" and the use of prohibited weapons in Ukraine. The strategic goals of the operation of these simulators are to replace the objective ideas of the target groups about the nature of the conflict with the "information phantoms" that the aggressor needs.

The introduction of alternative concepts, meanings and imitations has led to the fact that this hybrid method of war has divided public opinion in Ukraine into more pro-Russian or more anti-Russian. The decree on blocking Russian Internet resources theoretically confirms that war is a war in the media. If the media usually cover military operations, the battle of values will have the opposite picture. The armed forces complete an operations launched by the media. As a result, the citizens of Ukraine postponed the actions of the armed forces in the conflict zone in protest against their participation in hostilities.

The description of the famous Russian political scientist Yakovlev is also interesting. Reading Russian scientific articles for five years, Yakovlev noted with interest that the people who coordinate the introduction and interpretation of Russian news studied the same textbook (Zozulia, 2020; Kriesi, 2013). The human psyche is arranged as follows: as soon as the accusation becomes the subject of public discussion, its "supporters" and "opponents", "experts" and "sofa experts" inevitably appear. A "big lie" can cause deep emotional trauma for the listener or viewer, which will determine their point of view over a long period of time, which contradicts any arguments of logic and reason.

The "40 by 60" method was invented by Goebbels. It is to create media that cover 60% of their information in the enemy's interests. Having thus earned his trust, the remaining 40% they use for extremely effective, thanks to this trust, misinformation (Lilleker, 2006; Snyder, 2010). Instead of proving something, the information is presented as something obvious, self-evident, and therefore unquestionably supported by the majority of the population. Despite its apparent simplicity, this method is incredibly effective, because the human psyche automatically responds to the opinion of the majority, seeking to join it. However, it is important to remember that the majority must be overwhelming, and its support must be absolute and unconditional. If these conditions are met, the number of supporters of the "majority position" begins to grow gradually, but steadily and increases exponentially over time (mainly due to members of the lower social strata, who are most vulnerable to "joining influence" effect).

One of the classic ways to support the "absolute obviousness" approach is to publish the results of various surveys that demonstrate absolute social consensus on specific issues. "Black" propaganda technology does not require that these reports be in any way related to reality. A lot can be said about all these methods, because their list is huge. However, there are other important things. The method of "black" propaganda influences the audience through a deep psychological mechanism, so that the consequences of this influence cannot be eliminated by ordinary logical arguments. Usually, this is impossible for the joining effect not to occur. However, if these conditions are met, the number of supporters of the "majority position" begins to grow gradually but steadily, and increases exponentially over time (mainly due to members of the lower social strata, who are most prone to the "joining effect") (Lilleker, 2006; Popescu, 2015).

However, the information war, in which Ukraine is significantly weaker than Russia, is also important. Therefore, the following objectives are important: building the political culture of Ukrainians, influencing the public consciousness of the population by creating effective counter-myths, demythologising consciousness, including the population of Eastern and Southern Ukraine, systemic rational explanations, counterarguments, even humour, and, of course, building a single state positive myth.

Demythologisation of mass consciousness is possible on the basis of the evolutionary development of national and civic worldview, strengthening critical attitudes in society, development of independent media, raising the level of education of the population, changing the philosophy of life of the average Ukrainian and state elite.

All methods of special propaganda are united by a single goal. It is to weaken the enemy's army by introducing internal enmity, mutual hatred and distrust to each other. The result they lead to is the one they were created to achieve. However, mutual hatred and internal enmity do not arise in the enemy's army, but in the homes and families of citizens. It seems that special propaganda works against its own population even more effectively than against enemy soldiers. Probably because the civilian population, unlike the enemy soldiers, cannot defend themselves.

Over the last ten years, there have been countless discussions on the need to adopt the Information Code of Ukraine and determine its importance for lawful settlement of problematic aspects of information security. This code should be based on the concept of national information policy.

Conclusions

Modern democratic society is forced to find a balance between certain extremes. In order to protect their democratic values, centuries-old traditions and achievements in the field of human rights, European countries have to find ways to restrict freedom of speech in order to protect the foundations of a democratic political regime. In fact, the effects of information aggression far outweigh the capabilities of conventional weapons, and it encourages temporary restrictions on democracy in order to maintain democratic values in the future.

In this case, temporary restrictions on democracy should be seen as a way to preserve democratic traditions in the future. Democracy can be limited only to the period of eradication of threats to its further existence. At the same time, these measures can be applied only in countries with a stable democratic system that are able to resist the abuse of power by the ruling elite. On the one hand, there is no democracy without freedom of speech, while on the other hand, there is a danger of using freedom of speech to manipulate public consciousness.

Prospects for further research involve scientific substantiation of the creation of an effective mechanism for confronting information threats in different national contexts. It is important to analyse the needs of citizens, what information they choose, from what sources, standards of their reliability, which will affect the consciousness, emotional expression, the relationship between citizens and the media. In order to withstand misinformation and manipulation spread through social networks and other communication channels in such conditions, each state needs consolidation and trust in the government. On the other hand, a large-scale rapid-response information policy with the use of modern technologies is important. At the same time, citizens must properly filter information, think critically, analyse, pay attention to sources of information, media owners, because as awareness increases, manipulation decreases.

In addition, the possibility of imposing international sanctions in the field of information should be considered separately, namely: 1) the requirement for media companies to geocode their Internet content and encode Russian satellite TV channels; 2) a ban on European satellite/cable TV providers to provide services to media companies in countries that have not yet introduced geocoding of web content and encoding of satellite TV signals.

Bibliographic references

Akimenko, V. & Giles, K. (2020). Russia's Cyber and Information Warfare. Asia Policy, 15(2), pp. 67-75. https://doi.org/10.1353/asp.2020.0014.

Asri, M. A. S., & Sualman, I. (2019). The perception of young adults on credibility of Facebook as a source of political information and its effects towards their political behaviour. Journal of Media and Information Warfare, 12(1), pp. 33-72.

Barabash, V. V. & Kotelenets, E. A. (2016). Information war and mediascape: theoretical aspects of current change. FSBEI HE Penza State University. Retrieved from https://izvuz_gn.pnzgu.ru/gn14316.

Batyuk, V. (2017). The US concept and practice of hybrid warfare. Strategic Analysis, 41(5), pp. 464-477. Retrieved from https://www.tandfonline.com/doi/abs/10.1080/09700161.2017.1343235?src=recsys&journalCode=rsan20

Bennett, W., & Iyengar, S. (2010). The shifting foundations of political communication: Responding to a defense of the media effects paradigm. Journal of Communication, 60(1), pp. 35-39.

Bielawski, R., & Radomska, A. (2017). Selected models of information warfare in cyberspace. Security and Defence Quarterly, 14(1), pp. 35-50.

Bilan, M. (2016). Ukraine declares war on journalism. The New York Times. Retrieved from https://www.nytimes.com/2016/06/01/opinion/ukraine-declares-war-on-journalism.html.

Blank, S. (2016). Russia, hybrid war and the evolution of Europe. Second line of defense. Retrieved from http://www.sldinfo.com/russia-hybrid-war-and-the-evolution-of-europe

Bukkvoll, T. (2016). Russian special operations forces in Crimea and Donbas. Parameters, 46(2), pp. 13-21.

Calha, J. (2015). Hybrid warfare: NATO's new strategic challenge? Report to NATO Parliamentary Assembly, 7 April 2015. Retrieved from https://www.nato-pa.int/sites/default/files/documents/2015%20-%20166%20DSC%2015%20E%20BIS%20-%20HYBRID%20WARFARE%20-%20CALHA%20REPORT.docx

Cassiday, J. & Johnson, E. (2016). Putin, Putiniana and the Question of a Post-Soviet Cult of Personality. The Slavonic and East European Review, 88(4), pp. 681-707. Retrieved from https://www.jstor.org/stable/41061898?seq=1#page_scan_tab_contents

Decree of the President of Ukraine № 47/2017, On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 "On the Information Security Doctrine of Ukraine". President of Ukraine, Official online representation, February 25 2017. Retrieved from https://www.president.gov.ua/documents/472017-21374

Decree of the President of Ukraine №133/2017, On the decision of the Defense and National Security Council of Ukraine of April 28, 2017 "On the application of personal special economic measures (sanctions) and other restrictive measures", President of Ukraine, Official online representation, 15 th of May 2017. Retrieved from

https://www.president.gov.ua/documents/1332017-21850

Desouza, K. C., Ahmad, A., Naseer, H., & Sharma, M. (2019). Weaponizing information systems for political disruption: The actor, lever, effects, and response taxonomy (ALERT). Computers & Security, 101606. https://doi.org/10.1016/j.cose.2019.101606.

Dodonov, R. (2015). The process of pacification in Ukraine: Transdnistrian and Chechen options. East Ukrainian conflict in the context of global transformation. Vinnitsia: Nilan-LLC.

Easton, D. & Almond, G. (2016). Two political systems analysts. Awami Politics. Retrieved from https://www.awamipolitics.com/two-political-systems-analysts-david-easton-gabriel-almond-6765.html.

Galeotti, M. (2017). The 'Gerasimov doctrine' and Russian non-linear war. In Moscow's shadows. Retrieved from https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/

Gerbner, G. (2018). Violence and terror in and by media. University of Pennsylvania. Retrieved from http://web.asc.upenn.edu/gerbner/Asset.aspx?assetID=412

Hoffman, F. (2014). On not-so-new warfare: Political warfare vs hybrid threats. War on the rocks. Retrieved from https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/.

Kalpokas, I. (2017). Information warfare on social media: A brand management perspective. Baltic Journal of Law & Politics, 10(1), pp. 35-62. https://doi.org/10.1515/bjlp-2017-0002

Karber, Ph. (2015). Russia's hybrid war campaign, implications for Ukraine &beyond. Washington CSIS. Retrieved from https://www.csis.org/events/russian-military-forum-russias-hybrid-war-campaign-implications-ukraine-and-beyond

Kharytonov, E., Kharytonova, O., Tolmachevska, Y., Fasii, B., & Tkalych, M. (2019). Information security and means of its legal support. Amazonia Investiga, 8(19), 255-265. https://amazoniainvestiga.info/index.php/amazonia/article/view/227

Kriesi, H. (2013). Democracy in the age of globalization and mediatization (Challenges to Democracy in the 21st Century). Basingstoke: Palgrave Macmillan.

Kurian, G. T. (2011). Legitimacy. In The Encyclopedia of Political Science (pp. 946-947). Editorial: CQ Press. https://www.doi.org/10.4135/9781608712434.n891

Law No. 1207-VII. On ensuring the rights and freedoms of citizens and the legal regime in the temporarily occupied territory of Ukraine, Legislation of Ukraine, 2014. Retrieved from https://zakon.rada.gov.ua/laws/show/1207-18?lang=en#Text

Law No. 2163-VIII, On the basic principles of cybersecurity in Ukraine, Legislation of Ukraine, 2017, Retrieved from https://zakon.rada.gov.ua/laws/show/2163-19#Text

Lilleker, D. G. (2006). Key concepts in political communication. Sage. Retrieved from https://people.unica.it/fulvioventurino/files/2015/10/LILLEKER_Key-concepts-in-political-communication.pdf.

Pazyuk, A., & Mitsik, V. (2019). Global cybersecurity culture in the international discourse: values and principles. Bulletin of the National Academy of Leading Personnel of Culture and Arts, 2, pp. 103-107.

Popescu, N. (2015). Hybrid tactics: neither new, nor only Russian. ISS European Union. Retrieved from https://www.iss.europa.eu/content/hybrid-tactics-neither-new-nor-only-russian

Qureshi, W. A. (2019). Information Warfare, international law, and the changing battlefield. Fordham International Law Journal, 43, 901-937.

Saakov, V. (2018). An expert group has been set up in the EU to combat fake news. DW Made for minds. Retrieved from https://www.dw.com/uk/%D1%83-%D1%94%D1%81-%D0%B7%D0%B0%D0%BF%D1%80%D0%B0%D1%86%D1%8E%D0%B2%D0%B0%D0%BB%D0%B0%D0%B8/a-42151697

Simons, G. (2021). The evolution of regime change and information warfare in the 21st century. Journal of International Analytics, II(4), pp. 72-90.

Snegovaya, M. (2018). Russia report I. Putin's information warfare in Ukraine. Soviet origins of Russia's hybrid warfare. Washington, DC: Institute for the Study of War.

Snyder, T. (2010). Bloodlands: Europe between Hitler and Stalin. New York: Basic Books.

Stadnyk, A. (2017). Use of propaganda during information wars: nature, mechanisms and technologies of influencing public opinion. Grani, 20, 5(145), pp. 10-15.

Zozulia, O. (2020). Fake as a tool of information warfare. Legal newspaper online. Retrieved from https://yur-gazeta.com/publications/practice/inshe/feyk-yak-instrument-informaciynoyi-viyni.html