COMBATTING DISINFORMATION AND CYBER THREATS IN THE EUROPEAN UNION AND UNITED STATES: LESSONS FOR UKRAINE

Vladyslav Teremetskyi, West Ukrainian National University
Kseniia Tokarieva, National Aviation University
Iurii Dziuba, Yaroslav Mudryi National Law University
Nikolay Shelukhin, Mariupol State University
Oleh Predmestnikov, Western Ukrainian National University
Ulyana Parpan, Lviv Polytechnic National University

ABSTRACT

The article analyzes the main means of counteracting misinformation, disinformation and cyber threats used by the European and international communities. It is determined that the main challenges of our time, which exacerbate the problem of disinformation, are Russia's information policy and the COVID-19 pandemic. The main institutions and regulations of Europe, which are aimed at overcoming the spread of false information in the media, are analyzed. The experience of France is mentioned, which created a powerful legal mechanism to prevent misinformation and combat its manifestations. The current state of US information security and the effectiveness of the US policy of combating disinformation are described. Special attention is paid to the issues of media and cyber education of the population. The latest trends in the institutionalization of countering misinformation and disinformation in Ukraine and ways to improve the strengthening of information security in the country are studied. It is established that Ukraine, as a direct participant in the information war, is obliged to support and involve at the national level European initiatives to strengthen information security and cyber security. The first steps include updating the legislation on information, increasing the role of information security in national security acts, approving the Strategy for Counteracting Disinformation and the Strategy for Ensuring Information Security, and institutionalizing the fight against misinformation and disinformation.

Keyword: Disinformation, Misinformation, Cyber Threats, Information Security, Misinformation, Information Society, "Hybrid War", Infodemia, Mass Media

INTRODUCTION

Information war is not a new phenomenon for the modern world order. It requires fewer resources than traditional military conflicts, but the consequences of such confrontation are also quite devastating. From now on, the state's defense capabilities are measured not only by material resources, but also by resistance to foreign propaganda and disinformation, which can destabilize the political situation or change public opinion through manipulative operations.

The development of digital technologies gives everyone more and more opportunities to create, disseminate and receive information. At the same time, the risks of misuse of information are increasing, but democratic processes and the consolidation of states' efforts allow for effective modernization of the means to combat such phenomena. Modern challenges, such as, for example, COVID-19, are the tests of humanity’s ability to counter common civilizational threats, organize to solve pressing issues and draw the right conclusions (Teremetskyi et al., 2021), and require a rapid response of the authorities both in the direction of solving the problem and in the direction of providing information to society with reliable and substantiated facts about it. Misinformation as a phenomenon of the information environment is unlikely to disappear completely, but it is possible to minimize its impact on individuals and the state, to form an ideology of critical evaluation of any news and reports. Ukraine is at the center of a "hybrid war" where information has become a weapon, so studying the world's experience in combating misinformation and disinformation is a necessary tool in strengthening national security.

MATERIALS AND METHODS

The empirical basis of this article was the provisions of European and international law as well as national regulations. The theoretical basis of this article is domestic and foreign studies of the current state of legal regulation of misinformation and disinformation in the world and Ukraine, ways to close gaps in world policy to combat disinformation and institutionalize the fight against propaganda.

The research methods were selected according to the purpose, tasks, object and subject of the article. In the process of research general scientific and special research methods were used. The method of system analysis provided an opportunity to analyze the main causes and catalysts for the emergence and spread of misinformation. The comparative law method allowed us to consider the differences and similarities of the policy of combating disinformation in the member states of the European Union and the United States of America. The formal-legal method was used in the study of international documents and analytical reports on the implementation of countering disinformation. Logical methods and synthesis method were used in determining the main vectors of Ukraine's development in the field of informatization and writing their own conclusions.

RESULTS

European Trends in the Fight against Misinformation, Disinformation and Cyber Threats

These days information covers all areas of human social life. The formation of the information society in the world undoubtedly has many advantages: from the automation of many management processes to improving the quality of life in general. At the same time, the globalization of the information space and the informatization of society carry certain risks, the fight against which directly affects the security of individuals and the state. The terms "information war", "hybrid war" and "disinformation" have become commonplace. The issue of misinformation and disinformation has become more acute in recent years, due to the challenges of our time, which we will consider below. We will use two related, but different in meaning terms in our study:

1) Disinformation in the sense of intentional false information, manipulation of facts, propaganda; false information disseminated for the purpose of political subversion;
2) Misinformation in the sense of false information that is disseminated in everyday life, regardless of intentions to mislead (Gebel, 2021). Both of these phenomena are negative and provoke disastrous changes in society although different in nature and scale of impact on society.

One of such challenges should be recognized as Russian mass disinformation, which Ukraine has been fighting since March 2014 and around which the efforts of the world's leading states - the United States and the European Union (EU) - have been consolidated. The East Strat Com Task Force found in one of its comments that the "pro-Kremlin" disinformation campaign involves publishing a large number of materials in different languages in a large number of media (EU East Strat Com Task Force, 2017). Experts have identified disinformation as a non-military method of achieving political goals, and its goal is to weaken and destabilize Western nations. The main means of disinformation are: humiliation of persons, political organizations or intergovernmental organizations; dissemination of contradictory messages; establishing distrust in reliable sources of information, basic means of information, etc.

But this is not the only manifestation of disinformation that is of concern to the international community. It is important to spread fake news about coronavirus disease, which poses a great threat to public health. During the pandemic, the number of cases of public misrepresentation in the field of health care, cyber-attacks and illegal information operations about the causes of the virus, treatment protocols and vaccination has increased. Among the most well-known manifestations of false information, which have been refuted by medical experts and found no justification, are the following: alcohol and chlorine solutions treat coronavirus, the virus was invented by elites to reduce population growth, 5G technology will spread coronavirus and other conspiracy theories (European Commission, 2021). Dissemination of such information is dangerous because the level of perception of misinformation in the world remains high: individuals harm their own health by refusing medical care or using untested alternative treatments. World Health Organization Director-General Tedros Adhanom stressed the need to combat "Infodemia" - an excessive amount of information about the coronavirus, which makes finding a solution to the global problem more difficult (United Nations, 2020). "Infodemia" includes cyber-attacks aimed at damaging the information systems of medical institutions, selling counterfeit drugs, spreading false information about the virus, and so on.

It should be noted that there is no experience of pursuing a policy of absolutely successful counteraction to misinformation and disinformation in the world. At the same time, EU and Council of Europe member states are making great efforts to monitor the causes of disinformation and misinformation and to develop effective solutions to overcome this negative phenomenon. The greatest risk of being exposed to external political manipulation exists in countries that have weak institutions and a low level of confidence in their own or European governance. Deviations from democracy create vulnerabilities, which can be seen in Hungary, Slovakia, Latvia, Greece and other countries, and allow other countries to take destabilizing measures (Galeotti, 2017).

At the present stage of development of public relations, the strategic task for European states is to strengthen Russia's policy of counteracting misinformation. Anti-democratic propaganda, interference in the elections of other countries, outside influence on political decisions - the elimination of such negative phenomena requires many resources. First of all, it is the development of information security strategies at the national level of each state, the content of which should include tools to combat disinformation (Grebenyuk & Leonov, 2019). Organizations such as the European Union External Action, namely The East Strat Com Task Force, which we mentioned earlier, and The European Center of Excellence for Countering Hybrid Threats, have had a major impact on strengthening information security and the potential of counterintelligence strategies in Europe. The subject of their activities is to prevent the dissemination of false information and to counteract "hybrid" threats.

At the present stage of development of public relations, the strategic task for European states is to strengthen Russia's policy of counteracting disinformation. Anti-democratic propaganda, interference in the elections of other countries, outside influence on political decisions - the elimination of such negative phenomena requires many resources. First of all, it is the development of information security strategies at the national level of each state, the content of which should include tools to combat disinformation (Grebenyuk & Leonov, 2019). Organizations such as the European Union External Action, namely The East StratCom Task Force, which we mentioned earlier, and The European Center of Excellence for Countering Hybrid Threats, have had a major impact on strengthening information security and the potential of counterintelligence strategies in Europe. The subject of their activities is to prevent the dissemination of false information and to counteract "hybrid" threats.

In 2017, the East Strat Com Task Force launched the EU *vs* Disinfo project and the euvsdisinfo.eu website to respond to Russian disinformation affecting the EU and neighboring countries. The project aims to raise public awareness of false information and manipulation of the media. The project repository contains more than 6,500 examples of disinformation, and as of May 2021, about 4,400 examples of disinformation related to Ukraine have been registered. The most common disinformation clichés are reports of Ukraine's undemocratic or aggressive nature in the international arena (EU *vs* Disinfo, 2021).

The legal regulation of countering disinformation in Europe is quite diverse. In Resolution 2217 (2018) on Legal challenges related to hybrid war and human rights obligations, the Parliamentary Assembly of the Council of Europe stressed the need to develop democracy protection against information weapons, while maintaining media freedom (Parliamentary Assembly of the Council of Europe, 2018). It is established that the "hybrid war" has the main characteristic – "legal asymmetry". This is due to the fact that the subjects of hybrid attacks usually deny their participation, guilt and responsibility for the information operations and, as a consequence, seek to avoid the legal consequences of their actions. Gaps in legal regulation and features of different legal systems allow opponents of hybrid war to disguise their actions. But the Resolution emphasizes that difficulties in countering hybrid threats do not mean that hybrid wars take place in a legal vacuum - domestic and international law apply to them. Hybrid wars have nationwide negative consequences, so in the public interest, some countries violate basic human rights by taking steps to counter disinformation. To avoid such situations, the Parliamentary Assembly of the Council of Europe called on member states to refrain from hybrid war, to actively participate in international cooperation to identify hybrid enemies and develop appropriate legal regulations, to exchange information on this issue, to raise public awareness of hybrid threats. Implement the Convention on Cybercrime, etc.

In October 2018, the European Commission’s code of practice against disinformation was published, where the term “disinformation” is interpreted as obviously false or misleading, information that is disseminated for economic gain and deliberate misleading and threatens democratic processes and public goods. (European Commission, 2021). Given that the line between countering disinformation and harsh censorship is thin, the media is closely following new tools to combat false information and criticizing most of them. In order to avoid such clashes between states and the media, the Code distinguishes between disinformation and inaccurate advertising, errors, satire, etc., stating that the latter do not fall within its scope. The provisions of the act are aimed at reducing monetization and the amount of advertising of misconduct or concealment of information. The code has become a progressive step in the fight against disinformation, and its technology has been signed by leading technology companies.

The EU`s Action Plan against Disinformation duplicates the definition of the term “disinformation” set out in the above-mentioned European Commission’s code of practice against disinformation (European Commission, 2018). The introduction to the Plan states that more than 30 countries around the world are using widespread disinformation, even in their own countries, which is of concern to the European community. The response to disinformation sets out in the Action Plan is based on the following main pillars: enhancing the EU's capacity to detect, analyze and expose false information; strengthening coordination in response to destructive information; private sector mobilization; raising public awareness and resilience to information attacks. Countering disinformation is gradually becoming institutional in nature - in Germany, government agencies and agencies are involved in countering fake news programs; National Security Communications operates in the United Kingdom; in France, active activities are demonstrated by state institutions and public organizations (Makarenko, 2019). Thus, European efforts against the spread of disinformation include not only declarative instructions, but also practical recommendations and specific instructions, which are designed to consolidate the negative challenges that arise in the way of informatization of society.

Good cooperation and active monitoring in the field of counteracting misinformation have quite powerful information results. The Fifth set of reports "Fighting COVID-19 disinformation Monitoring Program" as of November 2020 outlined the following achievements of the signatories of the European Commission’s code of practice against disinformation: Google displays lists of permitted vaccines, YouTube plans to add reliable information on vaccination received from local authorities, Facebook should delete posts that contain false allegations of vaccination, refuted by medical experts, etc. (European Commission, 2020). World-renowned media, which are used by millions of people, have the ability to promote authoritative sources of information, limit the flow of disinformation (misinformation) and reduce the popularity of misleading information, which plays a crucial role in combating misinformation.

In the context of the study of the European experience in combating misinformation, mention should be made of France, which has relatively recently made substantial changes to its information legislation. In 2018, France adapted obsolete legal instruments in the field of information to modern digital technologies. The changes affected the activities of the above-mentioned online platforms and expanded the powers of the main regulator of information policy. The Conseil Supérieur de l'Audiovisuel (CSA) (The Conseil supérieur de l'audiovisuel, 2018). The Council may require information platforms to publish the names of subscribers to articles on the Internet and the funds they have spent on disseminating destructive information (Levush, 2019). The introduction of online platform reporting procedures to the Council and a public register for the identification of information promotion operations made France one of the first countries to create an effective and consistent legal mechanism to combat misinformation that threatens the information security of individuals, society and the state.

The new category of "cyber security" is also a strategic direction for the administrations of European countries, as fundamental human rights must be respected in all spheres of life, especially during digital data collection and processing on the Internet. Created by the Council of Europe in 2001, the Convention on Cybercrime raised the concerns of the European community about the risks of criminal offenses on computer networks (Council of Europe, 2001). The Convention is the beginning of an effective fight against cyber threats, as it aims to stop actions that threaten the confidentiality, accessibility and integrity of computer networks and data. The establishment of criminal liability for such actions, international cooperation and the fight against cybercrime at the international level are designed to prevent any abuse and respond quickly to their occurrence. In 2013, the EU cyber security strategy was published: An open, safe and secure cyberspace, and the main areas of work in the field of combating cyber threats in Europe were the creation of a network of EU operational security centers, the creation of a joint unit on cybernetics, Internet security standards. expansion of cyber diplomacy, reliable data encryption, etc. (Council of the European Union, 2021).

Countering Misinformation, Disinformation and Cyber Threats in the United States

The rapid development of information security in the United States has gone through several stages, including: 1939-1947 - the stage of emergence; 1947–1982 - stage of formation; 1983–2001 - stage of active development; since 2001 - to this day - a stage of radical improvement. US legal regulation in the field of information security is the legal basis of a unified state policy in the field of national security interests. An array of federal and state laws aimed at protecting information suggests that information security is a promising area of cooperation between Ukraine and the United States (Busol, 2017). The US information policy is quite successful, which is influenced by such factors as systemic legal regulation, international cooperation, successful policy of state institutions, public awareness, public confidence in government and the media. A separate guarantee of American information security is cyber insurance. US policy includes continuous monitoring of weaknesses in the state's information systems, implementation of effective national measures aimed at strengthening the security of cyberspace, quality education in the field of information and training in the field of cyberspace protection (Voznyuk & Nychyporchuk, 2018).

The United States suffers from constant cyberattacks by political opponents. At the same time, American cyberspace is the safest, which is the result of many years of work by the authorities in this direction. In May 2021, the Executive Order on Improving the Nation’s Cybersecurity was published, which aims to protect networks, infrastructure and the economy (The White House, 2021). The order provides for a Cyber Safety Review Board and the introduction of stricter cybersecurity standards.

Despite the generally recognized success in information security policy, the direction of counteracting US disinformation and misinformation remains a vulnerability of the country's national security. The report of the Atlantic Council Democratic defense against disinformation 2.0 in 2019 concluded that in the context of solving the problem of disinformation, the United States lagged behind the EU (Fried, 2019). Disinformation in the United States becomes especially relevant during elections, so the government's priority is usually to ensure the security of the election process, rather than overcoming disinformation in general. This approach may be too narrow due to the sporadic nature, but disinformation is a constant phenomenon. Disinformation exists outside of election cycles, so measures to strengthen resilience to the spread of fake news by foreign sources of information should be implemented consistently and consistently at the governmental level.

The information environment suffers from misinformation on a global scale, because the latest information and communication technologies simplify the process of spreading fake information. American society has simultaneously faced several powerful information challenges: the coronavirus pandemic, the presidential election, and the Black Lives Matter protests. In the early stages, the spread of COVID-19 became a major topic of discussion in the American media, displacing the presidential race. The emotional stress of the population due to fear for their health has increased the demand for information about the coronavirus. Meanwhile, widespread misinformation has unfolded: fake news has been circulating at an accelerated pace (Koshkin, 2020). Social changes in society took place against the background of cyclical fake news, and critical thinking or the availability of higher education did not protect citizens from the negative impact of misinformation. Instead, it once again demonstrated the importance of a policy of systematic counteraction to the dissemination of false information and the role of the media in social processes.

Jaiswal, LoSchiavo & Perlman point out that certain unresolved issues related to the spread of AIDS and racial prejudice affect the perception of the US population about coronavirus information (Jaiswal, LoSchiavo & Perlman, 2020) Distrust of the government is due to the belief that the US federal government was involved in the creation and spread of HIV as a form of genocide against black citizens. Populations of blacks and Latinos were disproportionately affected by COVID-19 infection, disproportionately arrested for physical disturbance, and were relatively less likely to be tested for COVID-19. Racism and systematic discrimination have led to high perceptions of misinformation. Therefore, accessible and impartial communication of important information by health professionals on the basis of equality is another way to combat misinformation in the United States, taking into account the epidemiological situation.

Despite the conclusion of the Atlantic Council and the crisis of the information environment, the United States has stabilized the processes against disinformation and continues to work in this direction. As in European countries, there is a systematic updating and filling of the regulatory framework for information. For example, the 2019 National Defense Authorization Act (NDAA) includes regulations on changes in the activities of the Global Engagement Center (United States Congress, 2018). The purpose of the Center is to direct, manage, synchronize, integrate, and coordinate the government's efforts to expose and counter disinformation and propaganda of other states aimed at undermining the policies and security of the United States and partner countries. The center should also monitor new disinformation trends to develop techniques to refute fake messages and promote credible, informed messages.

Noteworthy are the results of the Global Engagement Center, which in its Special Report: Russia’s Pillars of Disinformation and Propaganda from 2020 identified five pillars of Russian propaganda (Global Engagement Center, 2020). Among them: official state sources of information and communication; state media aimed at both domestic and foreign audiences; development of proxy servers; use of social networks; disinformation in cyberspace. The activities of major Russian media platforms and publications that spread disinformation about US policy were also covered. The report received criticism and attempts to refute its content by Russian politicians and experts.

Countering disinformation and misinformation in the United States has a special direction the development of children's media literacy. Every year, the number of resources for such development increases, so students in American schools is constantly gaining critical thinking skills for the objective perception of large amounts of information. The method of gamification allows you to absorb the necessary material at the subconscious level. In addition, it causes a relatively high interest of children and a high level of their concentration. Among the most effective programs that promote media literacy are: text online game Bad News, which increases psychological resistance to misinformation; online program Be Internet Awesome, one of the developers of which is Google, which demonstrates the techniques of misinformation and forms the habit of checking information; Bbc I reporter online learning game, where children play the role of journalists and decide which posts or photos on social networks can be trusted (Prikhodkina, 2020).

The Democratic Defense against Disinformation 2.0 report mentioned by us offers, in addition to the existing ones, new directions for the development of countering disinformation for the United States, to which Ukraine should also pay attention (Fried, 2019). The Atlantic Council calls on the United States to continue to impose sanctions on foreign disinformation providers and their sponsors. In addition, the institution recommends the introduction of a complex procedure for mandatory identification of bots. Given that the use of bots does not always pursue the goal of spreading disinformation, identification can only be assigned to foreign bots in compliance with the principles of transparency and integrity.

It can be concluded that the US experience is also valuable for Ukraine, because, despite the increased manifestations of disinformation, American society has a high level of trust in government and the media. Every citizen of a democratic state must have the ability to find unbiased sources of information and to distinguish between false information and journalism, so Ukrainian-American cooperation is a social need.

Ukrainian Experience and Prospects of Counteracting Disinformation and Cyber Threats

Ukrainian society today can observe that unregulated information relations create all the preconditions for new information totalitarianism. However, if for several years there was a corresponding threat of the transfer of virtual into real life; today we see all the manifestations of information war. The information space is the key to the country's development, as it can perform many tasks. In modern conditions, the Ukrainian information space is formed mainly under the strong influence of external and internal factors. These include the ongoing hostilities in the East, the economic crisis, the influence of international organizations on the resolution of the conflict in Ukraine, etc. (Sopilko, 2015).

The situation with disinformation in Ukraine corresponds to world trends on the one hand, and has its own specifics on the other one. In such an environment, when a pandemic significantly increases feelings of stress and anxiety, many recipients of information look for it in the language they know best. While the relevant Russian-language content is many times more. Other negative factors that allow the spread of Russian disinformation in Ukraine also include: intensification of the use of social networks; weak spread of critical thinking; traditional weakness of Ukrainian state institutions; emotional vulnerability of Ukrainian society due to armed conflict (Magda, 2020).

Given the concerns of the population and the negative consequences of disinformation in Ukraine, in 2020-2021 the authorities mobilized all forces to develop regulations to combat disinformation. In 2020, the presentation of the bill "On Countering Disinformation" took place. However, the content of the provisions of the draft law caused indignation on the part of both the domestic media and international organizations. The provision on the introduction of criminal liability for "systematic deliberate mass dissemination of knowingly unreliable reports of facts, events, phenomena that threaten national security, public safety, territorial integrity, sovereignty, and defense of Ukraine, the right of the Ukrainian people to self-determination, life and health" was debatable (Cabinet of Ministers of Ukraine, 2020).

A presentation on the social network Facebook was followed by a message from the UN Human Rights Monitoring Mission, in which the organization called on the authorities to refrain from imposing unnecessary restrictions on the media (UN Human Rights Monitoring Mission, 2020). Establishing criminal liability for disinformation can lead to mass harassment of journalists, as there is no clear distinction between critical journalistic activity and disinformation. Undermining media freedom and self-censorship violate international human rights standards, so the main task for the Ukrainian legislator remains to continue searching for the best option for balancing human rights and satisfying the public interest in combating false information.

The main problem of the internal organization of state and non-state institutions in combating the dissemination of false information in the information space is to achieve parity between the need to protect the right of citizens to receive reliable legal information, the right to freedom of speech and national interests of Ukraine. The existing imbalance is caused by the lack of effective mechanisms against misinformation and its dissemination through social networks. Involving only the European experience of combating disinformation through social media is not an effective measure of struggle, as Ukraine is in a special situation - military conflict and occupation regimes in parts of the territory. However, at the same time, the importance of fakes in social networks should not be underestimated, because they are the main intermediary between the customer of disinformation (misinformation) and users. The active dissemination of misinformation on social media is facilitated by their accessibility, convenience, diversity and ability to disseminate information quickly (Karpenko, 2021).

Despite outdated legislation in the field of information and the absence of a law on combating disinformation, institutional development in this direction is gaining momentum. Many years of activity, first of all, of public organizations, allowed Ukrainians to understand the scale of the disinformation campaign that has been launched against Ukraine since 2014. The main non-governmental organizations fighting in this area include the Media Reform Center with its Stop Fake project, the Institute for Regional Press Development and the Beyond News project, the Commission on Journalistic Ethics, and the Ukrainian Institute of Media and Communication. Human Rights Platform" and others (Burak, 2020). CSOs are full participants in information relations and information security, and the state, in turn, should provide financial support to such organizations, as their activities are related to the strategic direction of the country - national security.

In May 2021, the Center for Countering Disinformation of the National Security and Defense Council of Ukraine was established (The Parliament of Ukraine, 2021). The main tasks to be implemented by the Center include monitoring the Ukrainian information space, identifying existing and projected threats to information security, providing other bodies with analytical materials on disinformation, participating in the development of strategic communications and information security strategy, studying international experience and other tasks. To effectively counter propaganda and disinformation, as well as to prevent any attempts to manipulate public opinion. There are no punitive functions within the competence of the Center, but its powers include the ability to report violations in the information environment to the National Security and Defense Council of Ukraine, which is a progressive step towards strengthening information security in the country.

However destructive processes related to the dissemination of information are large-scale, the Center for Strategic Communications and Information Security at the Ministry of Culture and Information Policy of Ukraine (Cabinet of Ministers of Ukraine, 2021) was also established. International cooperation, namely regular notification of hybrid threats from Russia at the international level, and promotion of Ukrainian narratives will be the main activities of the newly created body.

The expediency of promoting Ukrainian narratives is explained as follows. The task of modern Russian propaganda against Ukraine is to discredit the Ukrainian people, their politics, economy and culture. The ultimate goal of Russian propaganda narratives is the psychological destabilization of Ukraine and the formation of the belief that Ukraine is a "failed state." The content of Russian media reports was actively accompanied by the preparation and conduct of a real "hot" war, hostilities, which led to numerous casualties, the destruction of economic sectors and a real threat to territorial integrity and sovereignty (Yuskiv, 2020). Therefore, Ukrainian narratives should displace Russian ones in order to deploy an active fight against the spread of fake messages.

So far, the creation of two institutions, which constitute the state mechanism for combating disinformation, raises many questions. The process of interaction or distinction between the spheres of activity of two seemingly similar institutions remains unclear. Also, in the framework of the legal regulation of their activities, the procedure for conducting examinations of information is not clear enough: how will the information be recognized as untrue one? Obviously, the heads of institutions will be able to provide answers to these questions only after the beginning of the implementation of their powers.

Regarding the prospects of counteracting disinformation in Ukraine, it should be noted that many steps have already been taken to meet the proper functioning of the information society. But there are still many gaps that need to be systematically and consistently filled in the light of international best practice. One of the important ways to revitalize the state is to take measures to prevent, detect and stop attempts by pro-Russian political groups to radicalize their own activities with the support of foreign sponsors. It is necessary to forbid in any way to inspire separatist sentiments and manifestations of religious hostility among ethnic groups. The development of high-quality independent journalism and the formation of a system of quality media education will stabilize the media space, where the media will participate in the fight against disinformation and misinformation (Grebenyuk & Leonov, 2019).

CONCLUSION

We can conclude that legal regulation is the main tool in the fight against disinformation and misinformation. The European experience in counteracting disinformation, misinformation and preventing hybrid threats is broader than in the United States. Ukraine, as a direct participant in the information war, is obliged to support and involve at the national level European initiatives to strengthen information security. The first steps should be updating the legislation on information, increasing the role of information security in national security acts, approving the Strategy for Counteracting Disinformation and the Strategy for Ensuring Information Security, improving the institutionalization of counteracting disinformation and misinformation, and so on. The low level of cyber security in Ukraine highlights the expediency of drawing on international experience in combating cyber threats and deepening the implementation of the provisions of the Convention on Cybercrime into national legislation.

Cyber security education programs need to be modernized on the model of a developed US education system. We should not forget that media education and raising the education of citizens form resistance to the dissemination of false information to the population, so these areas of work are also relevant for Ukraine. The policy course towards European integration requires the state to unconditionally respect and ensure fundamental human rights and freedoms, including the right to freedom of expression. Therefore, the future law on counteracting misinformation should contain a clear definition of "misinformation" and "disinformation", to distinguish it from other information phenomena in order not to violate the interests of the "fourth branch of government" - the media. Ukrainian journalists should not become opponents of the policy of counteracting disinformation, but its direct participants who will have the appropriate knowledge and skills to identify and expose false information.

REFERENCES

Burak, M.V. (2020). The potential of civil society in preventing misinformation. *Proceedings of the Inter university scientific-practical round table «Criminological Theory and Practice: Experience, Problems of Today and Ways of their Solution»*, 137-139.

Busol, O. (2017). US information security: Legislation and prospects for cooperation for Ukraine. *Social Communications Research Center*.

Cabinet of Ministers of Ukraine. (2020). The main provisions of the draft law on counteracting misinformation have been published.

Cabinet of Ministers of Ukraine. (2021). The center for strategic communications and information security was presented.

Council of Europe. (2001). *Convention on Cybercrime ETS No.185 Budapest*.

Council of the European Union. (2021). *Cybersecurity: Council adopts conclusions on the EU's cybersecurity strategy*.

EU East StratCom Task Force. (2017). *Means, goals and consequences of the pro-Kremlin disinformation campaign*.

European Commission. (2018). *Action plan against disinformation*.

European Commission. (2020). *Fifth set of reports – Fighting COVID-19 disinformation monitoring programme*.

European Commission. (2021). *Code of practice on disinformation*.

European Commission. (2021). *Tackling coronavirus disinformation*.

EU *vs* Disinfo. (2021). Deny, deceive, defame and deflect.

Fried, D. (2019). Democratic defense against disinformation 2.0. *Atlantic Council*.

Galeotti, M. (2017). Controlling chaos: How Russia manages its political war in Europe. *European Council on Foreign Relations, 228*.

Gebel, M. (2021). Misinformation *vs.* disinformation: What to know about each form of false information, and how to spot them online. *Insider*.

Global Engagement Center. (2020). *GEC special report: Russia's pillars of disinformation and propaganda*.

Grebenyuk, M.V., & Leonov, B.D. (2019). Problems of counteracting the spread of destructive propaganda and misinformation on the eve of the election: An analysis of the EU experience. *Information and Law, 2,* 82-89.

Jaiswal, J., LoSchiavo, C., & Perlman, D.C. (2020). Disinformation, misinformation and inequality-driven mistrust in the time of COVID-19: Lessons unlearned from AIDS denialism. *AIDS and Behavior, 24,* 2776-2780.

Karpenko, O. (2021). Development of strategic approaches and practical recommendations for counteracting the spread of mis information in Ukraine through social media. *Bulletin of the National Academy of Public Administration under the President of Ukraine, 1*(100), 7-14.

Koshkin, P. (2020). Information and political aspects of the coronavirus pandemic in the United States. *Paths to Peace and Security, 2,* 120-132.

Levush, R. (2019). *Government responses to disinformation on social media platforms: Argentina, Australia, Canada, China, Denmark, Egypt, European Union, France, Germany, India, Israel, Mexico, Russian Federation, Sweden, United Arab Emirates, United Kingdom*. The Law Library of Congress.

Magda, E. (2020). Covid-19 pandemic and disinformation campaigns: Case of Ukraine. *Visnuk of the Lviv University. Series Philos.-Political Studies, 30,* 176-182.

Makarenko, E.A. (2019). Countering Russian propaganda in the international arena: The European dimension. *Proceedings of the International scientific-practical conference «Deoccupation and reintegration of the information space of Crimea»*, 29-30.

Parliamentary Assembly of the Council of Europe (2018). *Resolution 2217 on Legal challenges related to hybrid war and human rights obligations*.

Prikhodkina, N.O. (2020). Gamification as an effective technology of students` media literacy development: US experience. *Collection of scientific works «Pedagogical sciences», 92,* 84-90**.**

Sopilko, I.M. (2015). Information threats and security of modern Ukrainian society. *Legal Bulletin Air and space law, 1*, 75-80.

Teremetskyi, V., Duliba, Ye., Didkivska, G., Maliarova, V., Kostenko, M., & Hrytsai, S. (2021). Responsibility for ensuring the world biosafety: Rethinking in the context of the covid-19 Pandemic. *Journal of Legal, Ethical and Regulatory Issues*, *24*(3).

The Conseil supérieur de l' audio visual. (2018). *Audio visual regulation missions*.

The White House. (2021). *Executive order on improving the Nation's Cybersecurity*.

UN Human Rights Monitoring Mission. (2020). *Disinformation must be combated, but not by restricting media freedom.* Facebook.

United Nations. (2020). UN tackles «infodemic» of misinformation and cybercrime in COVID-19 crisis.

United States Congress. (2018). *John S. Mccain national defense authorization act for fiscal year 2019 No. 115-232*.

Verkhovna Rada of Ukraine (2021). *Decree of the president of Ukraine on the issues of the center for countering disinformation*.

Voznyuk, Y., & Nychyporchuk, N. (2018). The secret of US success in the field of information security. *International relations, public communications and regional studies, 1*(3), 66-71.

Yuskiv, H. (2020). Rares of russian propaganda in Ukraine. *Visnuk of the Lviv University. Series Philos.-Political Studies, 30*, 226-232.