INFORMATION TERRORISM AND ITS PREVENTION IN THE GLOBAL POLITICAL ENVIRONMENT IN THE 21ST CENTURY

[a]SVITLANA VNUCHKO, [b]VIKTOR TEREMKO, [c]OLENA POLOVKO, [d]ANNA STYCHYNSKA

[a,b,c,d]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
email: [a]vnuchko@ukr.net, [b]v.teremko@gmail.com, [c]alenateze@ukr.net, [d]by_stycha@ukr.net

Abstract: The manifestations of information terrorism can be realized concerning the subjects of the global political sphere. Preventing and countering its consequences is a difficult task, primarily due to the multiple directions of modern threats, as well as the complexity of selecting and implementing measures to be taken to counter such manifestations of information danger. The study aims to analyze the trends in the development of measures to counter information terrorist attacks that have been and are being carried out against the targets of the global political sphere in the XXI century. The research was carried out using the methods of sequential analysis of the peculiarities of development and systemic description of information terrorism. In addition, the article provides a comparative assessment of related concepts. The descriptive method, comparison, analysis and synthesis of information were used to assess the content, methods of counteraction, principles and measures to counter information threats. According to the research results, the key features of countering information terrorism today include the formation and improvement of the regulatory framework based on global cooperation, openness, transparency, increased responsibility and proactive state policy to counter information terrorist attacks.

Keywords: Countering disinformation, Global political sphere, Information space, Information terrorism, Information threat, Means of protecting public political space.

1 Introduction

Information terrorism is a socio-political phenomenon and a threat to the interests of the individual, society, state in the global space. The use of science and technology by terrorists in the political space is aimed at spreading disinformation (biased, false, distorted) to manipulate public consciousness and intimidate for political purposes. Countering information terrorism in the political space is a complex global problem, often due to the existing asymmetry of threats and countermeasures. The Center for Countering Disinformation at the National Security and Defense Council of Ukraine (2022) defines disinformation as false information of a manipulative nature. Among the technologies is artificial intelligence, which is both a tool for malicious creation and large-scale dissemination of disinformation and an effective tool for detecting fakes and disseminating reliable information. Disinformation is not a new phenomenon in the information space. The use of propaganda and manipulation of facts originated with the first states and even then served as a weapon in political battles. Together with the evolution and globalization of information technologies, the loss of monopoly on information and the restructuring of the classical news hierarchy in favor of the Internet media, disinformation activities pose an even greater threat to the public consciousness, especially in the countries of "young democracy".

On January 29, 2019, the European Commissioner for Digital Economy and Society M. Gabriel during the presentation of the first report on the elimination of political disinformation on the eve of the elections reported that the fight against disinformation and propaganda in the EU's cooperation with Facebook, Google or Twitter has a number of shortcomings. Among the shortcomings, it was found that: 1) disinformation knows no borders, so a pan-European approach is needed, according to which all EU countries should cooperate in this area; 2) there is a delay in the reaction aimed at preventing disinformation, i.e. it is important that plans are implemented quickly enough; 3) it is necessary to expand the "field of action" in the field of transparency on the Internet in order to identify advertising that pursues hidden political goals. The above indicates the growing problems of countering information terrorism and the need to analyze the state of such counteraction.

The aim of the article is a comprehensive analysis of countering information terrorism in the global political space of the XXI century on the example of Ukraine.

2 Literature Review

In the work of Arquilla, Ronfeldt & Zanini (1999) the phenomenon of terrorism is considered as a shadow way of conducting asymmetric warfare by weak political leaders, for instance, religious fundamentalists, racist opposition, ethnic nationalists. Terrorism is a way of violence to achieve a new world order through the destruction of the existing one. In the information age, the motives of terrorism are similar, but its characteristics are different: the way of organization, doctrine, strategy, technology of use. Information terrorism is present in information networks through decentralized schemes to create arrays of transnational Internet groups. The doctrine and strategy involves moving into the information space and conducting tactical "information operations", using a rotation approach to information campaigns (Kravchenko et al., 2022; Kostetska et al., 2021). Advanced information technologies are used to conduct operations and support the organizational structure. Hence, Arquilla, Ronfeldt & Zanini (2000) described the concept of information terrorism. It has evolved into "network warfare" which is part of hybrid warfare (Post, Ruby & Shaw, 2000). Such warfare can be countered by creating inter-organizational networks within the armed forces and government. To counter it, it is advisable to create information weapons that will symmetrically respond to the threats of information terrorism at different levels of the global political space.

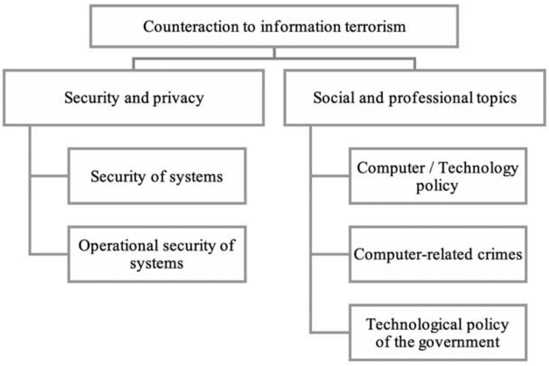

Counteraction to information terrorism
Security and privacy
Social and professional topics
Security of systems
Operational security of systems
Computer / Technology policy
Computer-related crimes
Technological policy of the government

Figure 1. Countering terrorism through information technology. Source: (Popp et al., 2004; Swire, 2006).

Countering information terrorism involves providing truthful, reliable, objective information about the possible risks of existing threats (Lemyre et al., 2006). For effective counteraction, a system of stakeholder interaction should be established to highlight the actual level of threats to different segments of the target audience (Lemyre et al., 2006). Countermeasures include analyzing the content of information, identifying weaknesses (vulnerabilities) in information delivery technologies, and developing appropriate responses to identified disinformation messages (Oh, Agrawal & Rao, 2011). As shown in Figure 1, countering terrorism through information technology includes: 1) security and privacy of information through security systems, including operational ones; 2) highlighting social and professional topics based on the developed policy of truthful information dissemination.

3 Research Methods

The article uses a mixed design to conduct a comprehensive study of countering information terrorism in the global political space. The mixed design included the following methods to fully cover the problem:

1. Sequence method for dividing the study of countering information terrorism into stages, each of which is based on the previous one. At the first stage, the legal framework for countering information terrorism in Ukraine and basic concepts and countermeasures have been studied. At the second stage, the key subjects of counteraction to information terrorism in Ukraine, their tasks and measures, principles and mechanisms of work have been investigated. At the third stage of the study the concept of information terrorism and its semantic field have been suggested.
2. The descriptive design was used to describe and collect additional information and answers to the questions of what constitutes "countering information terrorism"; where, when and how countering information terrorism takes place.
3. The systematic review was used to collect facts, evidence on countering information terrorism. Furthermore, it helped to analyze the available data on the strategy, principles, tasks, measures, tools, mechanisms of counteraction on the example of Ukraine.
4. The case method is used to analyze the counteraction to information terrorism on the example of Ukraine.

The source base of the research included materials, data and information of the Verkhovna Rada of Ukraine, the Ministry of Justice of Ukraine, the Center for Countering Disinformation, the National Security and Defense Council of Ukraine, the Ministry of Culture and Information Policy of Ukraine, the Center for Strategic Communications and Information Security.

4 Results

4.1 National legislation and information policy of countering terrorism

Regulatory legal acts in the information sphere of Ukraine, which are the basis of information policy and counter-terrorism, include Laws, Decrees of the President, Resolutions and Orders of the Cabinet of Ministers of Ukraine.
The Laws include the following:

- "On Information";
- "On Access to Public Information";
- "On Citizens' Appeals";
- "On Television and Radio Broadcasting";
- "On Printed Mass Media (Press) in Ukraine";
- "On Information Agencies";
- "On state support of mass media and social protection of journalists";
- "On the procedure for covering the activities of state authorities and local self-government bodies in Ukraine by the mass media";
- "On peculiarities of the state policy on ensuring the state sovereignty of Ukraine in the temporarily occupied territories in Donetsk and Luhansk regions";
- "On ensuring the rights and freedoms of citizens and the legal regime in the temporarily occupied territory of Ukraine";
- "On the adjacent zone of Ukraine";
- "On ensuring the rights and freedoms of internally displaced persons";
- "On Public Television and Radio Broadcasting of Ukraine" (Ministry of Justice of Ukraine, 2022).

The key strategic documents in the information sphere are the Presidential Decrees "On the Information Security Strategy" of 15 October 2021 and "On the Communication Strategy on Euro-Atlantic Integration of Ukraine for the period up to 2025" (Verkhovna Rada of Ukraine, 2022a; 2022b).

The Information Security Strategy (hereinafter – the Strategy) identifies current challenges and threats to the national security of Ukraine in the information sphere. It outlines strategic goals and objectives aimed at countering such threats, protecting the rights of individuals to information and personal data protection. The goal will be achieved by taking measures to deter and counter threats to the information security of Ukraine. In addition, it is important to neutralize information aggression, including special information operations of the aggressor state aimed at undermining the state sovereignty and territorial integrity of Ukraine. Therefore, it is necessary to ensure the information stability of society and the state, to create an effective system of interaction between public authorities, local governments and society. Attention should be paid to the development of international cooperation in the field of information security on the basis of partnership and mutual support.

Table 1. Challenges and threats to information security of Ukraine at the global, national levels

Challenges and threats	The list
Global challenges and threats	- Increasing number of global disinformation campaigns - Information policy of the Russian Federation is a threat not only for Ukraine, but also for other democratic states - Social networks as subjects of influence in the information space - Insufficient level of media literacy (media culture) in the context of rapid development of digital technologies
National challenges and threats	- Information influence of the Russian Federation as an aggressor state on the population of Ukraine - Information dominance of the Russian Federation as an aggressor state in the temporarily occupied territories of Ukraine - Limited capacity to respond to disinformation campaigns - Unformed system of strategic communications - Imperfection of regulation of relations in the field of information activity and protection of journalist professional activity - Attempts to manipulate the consciousness of Ukrainian citizens regarding the European and Euro-Atlantic integration of Ukraine - Access to information at the local level - Insufficient level of information culture and media literacy in society to counter manipulative and informational influences

Source: (Verkhovna Rada of Ukraine, 2022a).

Countering disinformation and information operations in Ukraine includes the following tasks:

1. Creation of a system for early detection, forecasting and prevention of hybrid threats, in particular, creation of a system for countering disinformation and information operations aimed at preventing, detecting and responding to information threats as quickly as possible;
2. Taking measures to prevent and counteract the spread of disinformation and destructive propaganda regarding Ukraine's European and Euro-Atlantic integration;
3. Development of the capabilities of the components of the defense forces to counter threats in the information space;
4. Preparation and conducting of information and psychological operations and other measures aimed at preventing, deterring and repulsing the armed aggression of the Russian Federation against Ukraine by the components of the defense forces;
5. Strengthening responsibility for the dissemination of false information (disinformation);
6. Introduction of effective mechanisms for detecting, fixing, restricting access to and/or removing from the Ukrainian segment of the Internet information, the placement of which is restricted or prohibited by law;
7. Effective interaction of state bodies, local self-government bodies and civil society institutions in the formation and implementation of state policy in the information sphere;

8. Preventing the distribution and demonstration of information and audiovisual products (products), holding touring events that popularize or promote the aggressor state and its authorities, representatives of the authorities of the aggressor state and their actions that create a positive image of the aggressor state, justify or recognize the legitimacy of the occupation of the territory of Ukraine, contain calls to overthrow the constitutional order, violation of the territorial integrity of Ukraine, propaganda of war, extremism, separatism, communist and/or national socialist (Nazi) totalitarian regimes and their symbols, violence, cruelty, incitement of national, interethnic, racial, religious enmity and hatred, committing terrorist acts, encroachment on human and civil rights and freedoms, etc;
9. Counteracting information campaigns aimed at attracting and/or involving Ukrainian citizens, including children, in paramilitary or armed groups not provided for by the laws of Ukraine.

To counter disinformation in Ukraine, national legislation also defines a number of prohibitions, requirements, and liability for violations of the law. Part two of Article 6 of the Law of Ukraine “On Television and Radio Broadcasting” (Verkhovna Rada of Ukraine, 2022c) prohibits the use of television and radio organizations, in particular, for unreasonable depiction of violence. It bans the spread of propaganda of exclusivity, superiority or inferiority of persons on the basis of their religious beliefs, ideology, belonging to a particular nation or race, physical or property status, social origin. Furthermore, broadcasting programs or their videos that can harm the physical, mental or moral development of children and adolescents, if they have the opportunity to watch them is forbidden. Distribution and advertising of pornographic materials and items is also against the law. One cannot spread the propaganda of narcotic drugs, psychotropic substances for any purpose of their use. The dissemination of information that violates the legitimate rights and interests of individuals and legal entities, infringes on the honor and dignity of a person; committing other acts that entail criminal liability is also against the law of Ukraine. Article 62 of the same Law establishes requirements for television programs and broadcasts to protect public morality and ensure the rights of minors and youth. According to Article 71 of this Law, responsibility for violation of the legislation on television and radio broadcasting is borne by television and radio organizations, program service providers, their managers and employees, other economic entities, officials of state authorities and local self-government bodies. Those guilty of violations bear civil, administrative and criminal liability in accordance with the legislation of Ukraine. The measure of responsibility and appropriate sanctions for violation of the legislation on television and radio broadcasting is established by the court. In cases specified by the Law, sanctions for violation of legislation on television and radio broadcasting are established by the National Council of Ukraine on Television and Radio Broadcasting. Decisions of the National Council on the application of penalties may be appealed in court.

Liability for violation of legislation on television and radio broadcasting is established on the basis of documentary evidence, acts of inspection of television and radio organizations, appeals of the state authorities defined by this Law.

Article 3 of the Law of Ukraine “On Printed Mass Media (Press) in Ukraine” (Verkhovna Rada of Ukraine, 2022d) also prohibits the use of printed mass media in Ukraine to disseminate information the disclosure of which is prohibited by Article 46 of the Law of Ukraine “On Information”. It prohibits the dissemination of calls for the seizure of power, violent change of the constitutional order or territorial integrity of Ukraine. Propaganda of war, violence and cruelty; incitement of racial, national, religious hatred is prohibited. The distribution of pornography and the use of disinformation for the purpose of committing terrorist acts and other criminal acts are not allowed. Part one of Article 41 of this Law stipulates that editorial offices, founders, publishers, distributors, state bodies, organizations and associations of citizens are responsible for violation of the legislation on print media.

According to part one of Article 15 of the Law of Ukraine “On the Protection of Public Morality”, state supervision over compliance with the requirements of this Law and current legislation in the field of protection of public morality is carried out within their competence by the Ministry of Culture and Tourism of Ukraine, the Ministry of Health of Ukraine, the Ministry of Justice of Ukraine, the Ministry of Education of Ukraine, the Ministry of Internal Affairs of Ukraine, the Prosecutor General’s Office of Ukraine, the State Customs Service of Ukraine, the State Committee for Television and Radio Broadcasting of Ukraine, the National Council of Ukraine (Verkhovna Rada of Ukraine, 2022e).

Based on the analysis of these provisions of the legislation, it can be concluded that today at the legislative level there is already a ban on the dissemination of “negative information” (i.e. information containing propaganda of violence, disinformation, other criminal acts), as well as responsibility for its dissemination.
In view of the above, the issue of ensuring the dissemination of “positive” information by the media can be solved in the following ways:

- ensuring coverage of the directions of the state information policy in the state mass media;
- formation, placement and execution of the state order for “positive” news, TV programs and broadcasts;
- ensuring public access to a wide range of mass media (domestic and foreign);
- bringing to responsibility for the content of TV programs and broadcasts that unreasonably show violence, contain videos that may harm the physical, mental or moral development of children and adolescents, including revocation of licenses.

4.2 Subjects of counteraction to information terrorism in Ukraine

The Center for Countering Disinformation (CCD) is a working body of the National Security and Defense Council of Ukraine (NSDC). It was established in accordance with its decision of March 11, 2021 "On the Establishment of the Center for Countering Disinformation", enacted by the Decree of the President of Ukraine of March 19, 2021 No. 106. The Center ensures the implementation of measures to counter current and projected threats to national security and national interests of Ukraine in the information sphere, ensuring information security of Ukraine, detecting and countering disinformation, effectively countering propaganda, destructive information influences and campaigns, preventing attempts to manipulate public opinion, and preventing the spread of false information. In its activities, it covers trends in informing about the state of military affairs, defense industry, the fight against crime and corruption, foreign and domestic policy, economy, critical infrastructure, ecology, healthcare, social sphere, formation of public consciousness, scientific and technological direction, etc. The main focus is on counteracting the spread of false information and combating information terrorism (Center for Countering Disinformation, 2022a).

In order to counteract information terrorism, the CCD performs a number of main tasks:

1. Analysis and monitoring of events and phenomena in the information space of Ukraine, the state of information security and Ukraine’s presence in the world information space.
2. Identification and study of current and forecasted threats to the information security of Ukraine, factors that influence their formation, forecasting and assessment of consequences for the security of national interests of Ukraine.
3. Provision of the National Security and Defense Council of Ukraine, the Chairman of the National Security and Defense

Council of Ukraine with information and analytical materials on ensuring information security of Ukraine, detection and counteraction to disinformation, effective counteraction to propaganda, destructive information influences and campaigns, prevention of attempts to manipulate public opinion.

4. Preparation and submission of proposals to the National Security and Defense Council of Ukraine, the Head of the National Security and Defense Council of Ukraine on:
   4.1. Defining conceptual approaches in the field of countering disinformation and destructive information influences and campaigns;
   4.2. Coordination of activities and interaction of executive authorities on national security in the information sphere, ensuring information security, detection and counteraction to disinformation, effective counteraction to propaganda, destructive information influences and campaigns, prevention of attempts to manipulate public opinion;
   4.3. Implementation of systemic measures aimed at strengthening the capacities of the security and defense sector entities and other state bodies to ensure information security, detect and counter disinformation, effectively counter propaganda, destructive information influences and campaigns, prevent attempts to manipulate public opinion, and develop national infrastructure in the relevant area;
   4.4. Improvement of the system of legal and scientific support of information security, detection and counteraction to disinformation, effective counteraction to propaganda, destructive information influences and campaigns, prevention of attempts to manipulate public opinion.
5. Participation in the development of the strategic communications system, organization and coordination of measures for its development.
6. Participation in the development and implementation of the Information Security Strategy of Ukraine, analysis of its implementation, in particular on the effectiveness of measures to counter disinformation.
7. Participation in the creation of an integrated system of information threat assessment and rapid response to them.
8. Development of a methodology for identifying threatening information materials of manipulative and disinformation nature.
9. Promoting cooperation between the state and civil society institutions in countering disinformation and destructive information influences and campaigns, organizing and participating in information and educational activities to increase media literacy of the society.
10. Study, summary and analysis of the experience of other states and international organizations in countering disinformation and preparation of proposals for its use in Ukraine.
11. Participates in determining priorities for attracting international technical assistance on information security, detection and counteraction to disinformation, effective counteraction to propaganda, destructive information influences and campaigns, prevention of attempts to manipulate public opinion.

The Ministry of Culture and Information Policy of Ukraine (2022) (MCIP) is a central executive body whose activities are directed and coordinated by the Cabinet of Ministers of Ukraine. The MCIP is the main body in the system of central executive bodies that ensures the formation and implementation of state policy in the spheres of information sovereignty of Ukraine (in terms of powers to manage the integral property complex of the Ukrainian National News Agency “Ukrinform”) and information security. MCIP is the main body in the system of central executive authorities that ensures the formation and implementation of state policy in the information and publishing sphere, in the field of television and radio broadcasting (Chyzhmar et al., 2019).

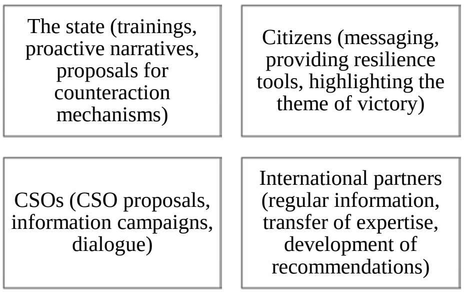
In March 2021, the Center for Strategic Communications and Information Security (CSCIS) was established at the MCIP. The work of the Center is focused on countering external threats, combining the efforts of the state and civil society organizations in combating disinformation, prompt response to fakes, as well as promoting Ukrainian narratives (2022a). Key tasks of the Center (2022a) are: 1) development of strategic communications (development of counter-narratives to the Russian Federation, conducting information campaigns, inclusion of Ukrainian narratives in the daily communication of the Government); 2) countering disinformation and building resilience to it. Constant notification of information attacks against Ukraine on the resources of the Center, in particular on the web portal, FB page, and Telegram channel; 3) raising awareness of hybrid threats (development and conducting trainings for civil servants, in particular for representatives of communication units); 4) regular reporting on hybrid aggression by Russia at the international level, development of mechanisms to counter disinformation together with international partners.

CSCIS (2022b) is one of the mechanisms to counter disinformation by joint efforts of the state and civil society. The Center’s work is focused on communication counteraction to external threats, in particular - information attacks of the Russian Federation. The main principles of the Center’s activity include constant cooperation with the public sector, the impossibility of political pressure, responsibility and openness. The main areas of work include (CSCIS, 2022b):

1. Development of strategic communications.
   1.1. Developing narratives to strengthen Ukraine's position on the issues that are most targeted by the aggressor.
   1.2. Development of messages for coordinated state communication.
   1.3. Combining the efforts of the state and the public sector for coordinated counteraction to disinformation.
2. Countering disinformation and building resistance to it.
   2.1. Creation of an online resource that will provide: response to information threats, a single database of the aggressor’s information presence, access to tools for building resilience, support for Ukrainian narratives.
   2.2. Conducting information campaigns.
   2.3. Formation of a public platform for discussing problems and developing solutions to counter disinformation
3. Joining forces with the world.
   3.1. Regular informing about the hybrid aggression of the Russian Federation
   3.2. Building cooperation with countries that have the same information threats as Ukraine.
   3.3. Development of mechanisms to counter disinformation together with partners.

For different types of target audiences, the CSCIS (2022b) carries out the following measures:

1. For the state: conducting trainings on raising awareness of hybrid threats, developing proactive narratives for state communications, proposals for mechanisms of systematic information on state counteraction to disinformation.
2. For citizens: reporting on information threats and mechanisms of malicious influence; providing tools to increase resilience to disinformation; highlighting Ukraine's victory in the information war.
3. For civil society organizations (CSOs): strengthening the voices of relevant CSOs by promoting their work; jointly conducting information campaigns and trainings; ensuring dialogue between the state and CSOs in the development of the legal framework.
4. For international partners: regular informing about the malicious activities of the aggressor; sharing the rich Ukrainian expertise in detecting and countering disinformation; joint development of recommendations on countering disinformation and building resilience to it.



The state (trainings, proactive narratives, proposals for counteraction mechanisms)

Citizens (messaging, providing resilience tools, highlighting the theme of victory)

CSOs (CSO proposals, information campaigns, dialogue)

International partners (regular information, transfer of expertise, development of recommendations)

Figure 2. Target audience of the CSCIS.
Source: formed by the author based on the data from CSCIS (2022b).

The system of counteraction to information terrorism and ensuring information security in Ukraine and abroad of the CSCIS includes the following key tools: analytics, monitoring, research and coverage of disinformation, its narratives and truthful information through various communication channels (official website, social networks, radio, television).

As a result of the study of information terrorism, the authors of this article propose the concept of information terrorism and the semantic field of disinformation. This concept defines the key notions related to information terrorism:

1. Propaganda – dissemination of political knowledge through various forms of communication to form the necessary worldview in the political space.
2. Disinformation narrative – a set of interconnected distorted, false facts, events, impressions, presented and ordered in a certain way to manipulate consciousness.
3. Disinformation – false, biased, distorted information of a manipulative nature to create reality.
4. Fake is an imitation of news, distorted presentation of information in order to manipulate consciousness.

These concepts are both similar and differ from each other in a number of characteristics, forming the concept of information terrorism at their intersection.

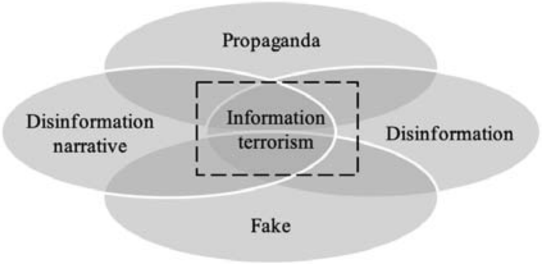


Figure 3. The concept of information terrorism and the semantic field of disinformation
Source: developed by the author.

5 Discussion

Powers of the security sector bodies of Ukraine to counter disinformation. There are reasons for this. Firstly, disinformation messages (fakes) are not illegal in essence. Secondly, disinformation is a term and method that was inherent in the activities of special services during the Cold War. Thirdly, the legislation of Ukraine is based on the fundamental principle of freedom of speech and does not criminalize the deliberate dissemination of false information to achieve political, economic, military and other goals by state and non-state actors. Finally, the recently established Center for Countering Disinformation at the National Security and Defense Council of Ukraine (NSDC) will soon establish cooperation with state authorities, law enforcement and intelligence agencies in order to implement the relevant Regulation.

The well-established scheme of information processing, distortion and manipulation of facts allows to hyperbolize or bring to absurdity important issues and facts for the society, forcing the population to reorient to local problems and eliminates any attempts to find alternative data. It is quite obvious that in order to establish communicative interactions, to secure the information space, the authorities need to work equally with both classical media and Internet resources. Improvement of the legislative framework and borrowing the experience of European countries will allow to more effectively implement the policy of countering information aggression. In our opinion, a necessary step is also to comprehensively inform the society about the basics of fact-checking, to interact with leading European media to borrow their experience and, in the long run, to create a specialized agency for information control. Regarding the latter, it would be advisable to inform the public in advance and coordinate actions with the media to avoid conflicts of interest and infringement of press freedom.

6 Conclusions

In Ukraine there is a dynamic development of the legal framework for the protection of the information sphere based on the principles of cooperation, responsibility, openness and transparency. This is the basis of information policy and counter-terrorism. Counteraction is carried out to overcome key global and national risks in close cooperation with international partners. The following components have been identified within the counteraction system: systems of early detection, forecasting and prevention of hybrid threats; measures to prevent and counteract the spread of disinformation; preparation and conduct of information and psychological operations by the components of the defense forces; strengthening responsibility for the spread of disinformation. Four target audiences and relevant tools for countering disinformation were identified: 1) the state (trainings, proactive narratives, proposals of countermeasures); 2) citizens (messages, provision of resilience tools, coverage of the topic of victory); 3) public organizations (CSO proposals, information campaigns, dialogue); 4) international partners (regular information, transfer of expertise, development of recommendations). As a result of the study of information terrorism, the authors of the article proposed the concept of information terrorism and the semantic field of disinformation. This concept defines key concepts related to information terrorism: propaganda – the dissemination of political knowledge through various forms of communication to form the worldview required in the political space; 2) disinformation narrative – a set of interconnected distorted, false facts, events, impressions, presented and ordered in a certain way to manipulate consciousness; disinformation – false, biased, distorted information of a manipulative nature to create reality; fake news is an imitation of news, a distorted presentation of information in order to manipulate consciousness.

Literature:

1. Arquilla, J., Ronfeldt, D., & Zanini, M.: *Networks, netwar, and information-age terrorism*. Naval Postgraduate School Monterey Ca Graduate School of Operational and Information Sciences, 1999.
2. Arquilla, J., Ronfeldt, D., & Zanini, M.: Information-age terrorism. *Current History*, 2000, *99*(636), 179-185.
3. Center for Countering Disinformation. About the Center’s activities, 2022a. https://cpd.gov.ua/documents/про-центр/
4. Center for Countering Disinformation. On propaganda, 2022b. https://cpd.gov.ua/warning/rosijska-propaganda-v-ukrayini-shho-vid/
5. Center for Strategic Communications and Information Security, 2022a. https://mkip.gov.ua/content/centr-strategichnih-komunikaciy-ta-informaciynoi-bezpeki-pri-ministerstvi-kulturi-ta-informaciynoi-politiki.html
6. Center for Strategic Communications, 2022b. https://spravdi.gov.ua/pro-nas/
7. Chyzhmar, K., Kolomiets, T., Dniprov, O., Sydorov, O., Rezvorovich, K.: The peculiarities of the legal regime of information in the e-declarations of persons authorized to perform the functions of state or local self-government. *Journal of Legal, Ethical and Regulatory Issues*. 2019, 22(5). https://www.abacademies.org/articles/the-peculiarities-of-the-legal-regime-of-information-in-the-e-declarations-of-persons-authorized-to-perform-the-functions-of-state-8613.html
8. Devost, M. G., Houghton, B. K., & Pollard, N. A.: Information terrorism: Political violence in the information age. *Terrorism and Political Violence*, 1997, *9*(1), 72-83.
9. Kostetska, K., Gordiichuk, Y., MovchaniukA., Vdovenko, N., Nahornyi, V., & Koval, V.: Inclusive development of social entrepreneurship in nature management. *Journal of Geology, Geography and Geoecology*, 2021, 30(3), 500-511. https://doi.org/https://doi.org/10.15421/112146
10. Kravchenko, T., Borshch, H., Gotsuliak, V., Nahornyi, V., Hanba, O., & Husak T.: Social Responsibility of the Government in the Conditions of the Global Pandemic Crisis. *Postmodern Openings*, 2022, 13(1), 468-480. https://doi.org/10.18662/po/13.1/408
11. Lemyre, L., Turner, M. C., Lee, J. E., & Krewski, D.: Public perception of terrorism threats and related information sources in Canada: implications for the management of terrorism risks. *Journal of Risk Research*, 2006, *9*(7), 755-774.
12. Ministry of Culture and Information Policy of Ukraine. About the Ministry, 2022. https://mkip.gov.ua/content/pro-ministerstvo.html
13. Ministry of Justice of Ukraine. Legal support of the state information policy, 2022. https://mkip.gov.ua/content/normativnopravovi-akti-v-informaciyniy-sferi.html
14. Oh, O., Agrawal, M., & Rao, H. R.: Information control and terrorism: Tracking the Mumbai terrorist attack through twitter. *Information Systems Frontiers*, 2011, *13*(1), 33-43.
15. Popp, R., Armour, T., Senator, T., & Numrych, K.: Countering terrorism through information technology. *Communications of the ACM*, 2004, *47*(3), 36-43.
16. Post, J. M., Ruby, K. G., & Shaw, E. D.: From car bombs to logic bombs: The growing threat from information terrorism. *Terrorism and Political Violence*, 2000, *12*(2), 97-122.
17. Swire, P. P.: Privacy and information sharing in the war on terrorism. *Vill. L. Rev.*, 2006, *51*, 951.
18. Verkhovna Rada of Ukraine. On the decision of the National Security and Defense Council of Ukraine of 15 October 2021, 2022a. https://zakon.rada.gov.ua/laws/show/685/2021#Text
19. Verkhovna Rada of Ukraine. On the Strategy of Communication on Euro-Atlantic Integration of Ukraine for the period up to 2025, 2022b. https://zakon.rada.gov.ua/laws/show/348/2021#Text
20. Verkhovna Rada of Ukraine. Law of Ukraine “On Television and Radio Broadcasting” 3759-XII of 07.10.2022, 2022c. https://zakon.rada.gov.ua/laws/show/3759-12#Text
21. Verkhovna Rada of Ukraine. Law of Ukraine “On Printed Mass Media (Press) in Ukraine” 2782-XII of 12.06.2022, 2022d. https://zakon.rada.gov.ua/laws/show/2782-12#Text
22. Verkhovna Rada of Ukraine. Law of Ukraine “On Protection of Public Morality” 1296-IV of 13.04.2022, 2022e. https://zakon.rada.gov.ua/laws/show/1296-15#Text

Primary Paper Section: A

Secondary Paper Section: AD, AJ, BD