THE IMPACT OF THE 4.0 TECHNOLOGICAL REVOLUTION ON THE HYBRID WAR OF THE RUSSIAN FEDERATION IN UKRAINE

[a]ANTONINA SHULIAK, [b]YEVHENIIA VOZNIUK, [c]IRYNA PATLASHYNSKA, [d]LESIA KACHKOVSKA, [e]SVITLANA GAVRYLIUK, [f]OREST SOROKOPUD

[a-f]Lesya Ukrainka Volyn National University, 13, Voli Ave, 43025, Lutsk, Ukraine
email: [a]antonina.mytko@vnu.edu.ua,
[b]voznyuk.yevhenija@vnu.edu.ua,
[c]iryna.patlashynsyka@vnu.edu.ua,
[d]kachkovska.lesja@vnu.edu.ua, [e]gavryliuk.svitlana@vnu.edu.ua,
[f]sorokopud.92@gmail.com

Abstract: The authors analyze the impact of the 4.0 technological revolution on the development of russia[1] hybrid war in Ukraine. The article examines the confrontation in frames of 4.0 technological revolution during the Fourth Generation Warfare (4GW), characterizes the hybrid warfare types and the impact of 4.0 technological revolution on each aspects. It is proved that hybrid warfare occupies an important place in the state domestic and foreign policies. Now it is gaining new importance in the information age. It is noted that, due to the development of new technologies, hybrid wars have become one of the most effective methods in achieving the goals. The modern hybrid war of the Russian Federation against Ukraine is monitored. It is emphasized that the formation of a single global information space, being a natural result of the world scientific and technical thought development as well as the improvement of computer and information technology, creates the preconditions for the development and use of information weapons. Both an effective information weapons possession and means of protection against them is becoming one of the main conditions for ensuring the national security of states in the 21st century. It is an instrument in the Russian-Ukrainian confrontation. The created information troops in Ukraine have become a community of active Ukrainians united to protect Ukraine from aggressive information propaganda of russian special services and to monitor information provocations against Ukraine, the russian media lies, and counter-propaganda spread.

Keywords: Hybrid war, 4.0 Technological revolution, Ukraine, russian federation, Misinformation, Manipulation, War.

1 Introduction

The relevance of the topic is determined by the fact that information can simultaneously contribute to stability in the state, its socio-economic and political development, but also pose a threat to the national interests of the state. Digital technologies are entangled in the structures of society. The dynamics of information transfer has changed greatly. Klaus Schwab claimed in 2016 that we are already facing artificial intelligence such as autonomous machines, drones, virtual assistants, translation programs, and advisor programs. The constant growth of computing power and ever-increasing amounts of data have allowed making increasingly more breakthroughs in the creation of artificial intelligence over the past few years: there are programs that develop new drugs, new algorithms and predict new trends in culture [24].

A significant percentage of the world population today uses social networks and media to communicate, learn and disseminate information. This should strengthen intercultural ties and cooperation, but freedom of information also leads to rising unsupported expectations, a lack of understanding of success criteria for groups and individuals, and the spread of extremist ideas and ideologies. In the current conditions of the Russian-Ukrainian war, Ukraine should take a more careful and balanced approach to protect the national information space, in particular, to take care of information hygiene. That is why strategic communications of the state as sovereign, democratic, legal as well as economically stable member of international relations are to be directed to assure national information security of all subjects to information relations and to institutionalize the process of keeping information hygiene. The special situation needs rapid and effective decisions in a course of the hostilities that are currently underway in Ukraine and represent the result of russian aggression.

[1] Since February 24, 2022 spelling of words «russian federation», «russia», vladimir putin in lowercase letters is common in Ukraine to emphasize the contempt to the aggressor and occupier.

2 Materials and Method

To solve a set of tasks, the following approaches such as interdisciplinary, complex and system-synergetic ones considering the modern paradigm of national information security in dialectical unity with the state information policy and introduction of an effective system of strategic communications at micro-, mezzo- and macro-levels are used. The chosen methodology of conducting the investigation combines and applies the following methods and approaches such as network analysis, systematic, integrated and civilizational research approaches, system analysis, systematization and classification methods as well as analysis of synthesis, objectivity, generalization, analogy, case-study, and others. The integrated approach fostered the identification of information intervention trends and patterns, anticipation of the consequences and possible developments of political events taking into account the peculiarities of geopolitical rivalry. The structural and functional approach involves research in terms of the interconnectedness of the elements that make up its structure and the functions inherent in all elements. Political-system analysis provided an opportunity to explore comprehensively the political space as a system of communicative relations.

The authors of the article are scholars of the International Relations Faculty at the Lesya Ukrainka Volyn National University and have long studied the impact of the 4.0 technological revolution on the development of Ukraine and Ukrainian foreign policy. In 2012-2014, they conducted a research “Information and Communication in the Modern World” (State Registration No.112U001779). In 2013–2015, the research topic was “Information Support of Cross-border Cooperation in Ukraine (State Registration No. 0113U002221), in 2018–2019 – “Information War as a New Dimension of Geopolitical Rivalry” together with the Institute of Security Sciences at the Krakow Pedagogical University) (State Registration No. 0119U001621). Currently, they are working on the topic within the Scientific Research Work “Information Hygiene as a Direction of National Security” (State Registration No. 0120U104944).

3 Results and Discussion

4.0 Technological Revolution vs Fourth Generation Warfare (4GW)

Technologies that have emerged at the intersection of the physical, digital, and biological worlds have led to the creation of new platforms through which citizens can communicate their views to the government, coordinate actions, and even avoid the attention of the authorities. At the same time, states have gained new tools to control the population based on a widespread surveillance and power over the digital infrastructure. The ability of states to change has become a matter of the survival. If they accept a new, transparent, ever-changing world, they will survive. By refusing to change, they doom themselves to growing internal conflicts. The fourth industrial revolution accelerated development so much that the old methods of regulation simply do not keep up with the current and new technologies today.

Currently, we can say with confidence that the 4.0 technological revolution gave rise to the Fourth Generation Warfare (4GW), to a conflict characterized by blurring the distinction between direct warfare and politics, between the military and civilians involved [22]. The idea of the Fourth Generation War was originated during the Cold War when the Soviet Union and the United States realized that large-scale use of tanks, aircraft, and missiles in these conditions is ineffective in the struggle for presence in different parts of the world. The role of guerrillas and various political, economic, financial, informational and psychological subversive operations has increased dramatically. In 1989, the American military expert W. Lind introduced the 4GW concept.

He believed that the Fourth Generation War was characterized by decentralization and the disappearance of the state's monopoly on war. This is what makes it possible to return to the war of cultures when immigration and multiculturalism create the preconditions for a war of identities [22].

Such war type is considered effective in terms of “cost-benefit”. In 2014-2022, russia did not invest huge sums in large-scale war, but used various latest subversive tactics to force the victim country to constantly exhaust its military, financial resources in the course of continuous and constantly externally fueled guerrilla warfare and terrorist activities. At the same time, the socio-economic chaos in the country was purposefully initiated to intensify psychological and informational pressure on Ukrainians and to push the undesirable power as the aggression object to be ready to surrender and leave.

Technological breakthroughs have potentially reduced the risk of hostilities by creating defense systems or increasing the accuracy of weapons. Namely during the Russian-Ukrainian war, unmanned aerial vehicles are used (or “drone” referring to an aircraft platform with additional equipment, that can be used interchangeably with terms such as BSP (drone), UAV (unmanned aerial vehicle)), which are designed to collect and provide information using on-board devices. They can be controlled from anywhere through using existing communication technologies (radio, microwave, satellite, optical, etc.). They can move along a predetermined route or between certain points with different levels of autonomy (independent choice of route, avoiding designated areas, identifying and avoiding both natural and civil threats, and others). Depending on the installed equipment, drones can perform image recognition (photo, video, infrared or thermal imaging, radar), electronic (radio monitoring), and the collected information can be transmitted in real time via wireless lines for operators, headquarters, and operational departments in the area. They are so small in size that they can start directly from the ground or small pneumatic launchers as well as the operator's ejection. Their main task is to monitor and track them in real time, so they can support the operation of the battalion in the given area [15; 23].

Increasingly, the 4.0 technological revolution is leading to asymmetrical warfare as a war characterized by significant differences in military power or the ability of participating countries to use strategies and tactics. In such a conflict, the resources of both sides differ significantly and during the struggle, the opponents try to use each other's characteristic shortcomings [22]. In 2001, the US Institute for Strategic Studies defined “asymmetry” as a strategic concept in the military and national security and the ability to act, organize, and think differently from opponents in order to maximize one's own strengths and vulnerabilities, seize initiative, or ‘conquire’ initiative space for maneuvering. Andrew Mack introduced the term “asymmetrical war” in 1975 in the article “Why Great Nations Lose Small Wars?” in magazine “World Politics”. The word “asymmetrical” was simply explained as the significant difference in strength between the various parties to the conflict (“strength” in such sense meant material force such as a large army, the latest weapons, a developed economy, etc.). In the 1990s, the special research was conducted based on the E. Mack concept. The U.S. military has been conducting a thorough analysis of the asymmetric wars issues since 2004. The traditional war involves at least two professional armies with roughly the same experience, resources, and technology. The only real difference is how they implement their strategies. Such a war is called symmetrical, because both sides are essentially the same. For example, when the Allies fight against the Axis powers, it was a conflict between professional, national armies that were mostly similar [16].

An information warfare as variety of modern wars is a form of information confrontation between different actors (states, non-governmental, economic, and other structures). It involves an implementation damage complex to the information sphere of the competing party and protection of own information sphere, as well as actions taken to achieving information advantage by harming information processes based on the very information and the information systems of the enemy while protecting own information [15; 23]. Blocking or distorting information flows and decision-making processes of the enemy are the main methods of information warfare [27]. The Chinese military leader Sun Tzu was the first to use the term “information warfare” in 1985. He attempted to generalize the experience of informational influence on the enemy. The concept of “information warfare” was introduced into scientific use by the American researcher M. McLuhan.

NATO uses the term iWar (information warfare) to describe a form of cyber warfare involving attacks on the Internet that target consumer Internet infrastructure, such as websites that provide access to online internet banking services. In this sense, iWar is different from cyber warfare, cyberterrorism, information warfare, or information warfare involving the use of computers, the Internet, and other means of storing or disseminating information to attack enemy information systems by using teleinformation systems and networks relating to communications control by access to military and critical infrastructure, electronic espionage, and battlefield command and control. The communications networks and satellite reconnaissance are their battlefields [12; 31].

Researchers [6] have identified the following five characteristics of iWar indicating that it can revolutionize conflict such as the potential for expanded offensive action, geographical coverage, difficulty of exposure (recognition), ease of spread and impact on “ready” goals. These qualities suggest that the advent of iWar could mean a new military revolution along with the invention of gunpowder or the atomic bomb.

One of the main information warfare objects is ideological and psychological environment of society associated with the use of information. Information resources and information infrastructure influence the psyche and behavior of people as well as resources that reveal the spiritual, cultural, historical, national values, traditions, heritage of the state, and nation in various spheres of society. Information infrastructure - namely all intermediate links between information and people and a system of public consciousness formation - is viewed as information warfare object too together with a system of public opinion formation and a system of development and decision-making, human consciousness and behavior.

Psychological warfare, cyber warfare; network war, ideological war, electronic warfare as types of information warfare can manifest in the following ways when television and radio broadcasting can be suppressed: television and radio resources are seized for misinformation; communication networks are blocked or inaccessible; stock exchange operations are sabotaged by means of electronic interference through information leaking or spreading misinformation [19].

Media warfare being a type of information war can be considered in two aspects. The former is a phenomenon of negative attitude in the media audience to the enemy (subject of international relations or participant in the political process within the country). The latter is the widespread use of media as a factor influencing the enemy to achieve the necessary political or military advantages and encouraging the adoption of favorable decisions for the initiator of the information impact, to affect human consciousness resulting in performance of the necessary actions [20]. Media war is a form of war lasting unofficially, even in clearly peaceful conditions. Each country tries to make the most of the media to achieve its political goals. The main “soldiers” of the media war are publicists, international propaganda experts and media agents. Media war requires closer cooperation and coordination from the country's military, political, information, security, media and advertising sectors [13].

The main goal of the media war is to create chaos when it becomes unclear who is a friend, who is an enemy, who has won the war and who has lost. The typical war methods are hiding real events and the real state of affairs and taking phrases out of

context followed by focusing on them. It is achieved through identification of negative aspects of a certain phenomenon with the phenomenon itself and its essence and hanging label. One of the methods is defamation, namely insult or ridicule of a person, people, emphasizing the personal traits of the opponent, spreading gossip, rumors, etc. It also includes involvement of persons in the situation which they are not involved in at all, suggesting to the opponent feelings of anxiety, depression, sometimes leading to complete despair and suicide [17].

Unresolved domestic problems and the desire to unite the country's population against an external enemy are often the main causes of media warfare, thereby diverting attention from domestic problems. Such type of war affects the mentality and behavior of people, stimulates radical sentiment in society. The main means of media war are radio, television, websites, the press. Hybrid warfare is known to have no rules. The tactics are flexible and are planned under the strategy of information war rather than frontal warfare, where an alternative reality is built, within which it is possible to turn an opponent into an enemy. The main and managing component of hybrid warfare is information warfare taking on today a new, modified form and emerging as a network-centric warfare. Under such concept, we understand the war of the new generation, in which the modeling and programming of the necessary processes in the enemy state is carried out by means of informational influence [4].

The object of network-centric warfare is mass and individual consciousness. Information influence can be carried out both against the background of information noise and in the information vacuum. Information and network warfare is built on the same principles as any advertising campaign, but its task is to 'sell' the idea of a hybrid aggressor. The attack is not aimed at the body, but at the soul of the enemy, because the strongest conflicts in human history, as it is known, were basically religious in nature. Therefore, network information warfare is a strong part of hybrid warfare [4].

Analysis of the most famous international military, political, and economic conflicts in the late 20th − early 21st centuries testified that information and psychological weapons as one of the means of hybrid warfare should be equated with weapons of mass destruction. Without killing physically, psychotechnologies become the cause of group as well as mass mental disorders that lead to social conflicts. Information impact on the population is carried out through various channels of information transmission such as the Internet, media, television, software, and more. Computers and information systems are affected by information warfare. In the information and psychological war, the informational direction is joined by the psychological one, in which the object of influence is individual and mass consciousness [18].

In the format of using the full range of information and psychological operations, social online networks have the opportunity to coordinate protest and terrorist movements. They are capable of dissemination of content related to information weapons, gathering important information of interest to the aggressor, tracking public sentiment and localization of information sources that pose a danger [14].

Thus, hybrid warfare occupies an important place in the domestic and foreign policies of states, and now it is gaining new importance in the information age. Due to the development of new technologies that have accelerated the spread of globalization processes and contributed to the creation of a single information space, information wars have become one of the most effective methods of achieving the goal. The use of information warfare as a means of geopolitical confrontation can be seen in the wars in the Persian Gulf, Chechnya, eastern Ukraine and Crimea, and Syria. Therefore, the study of this phenomenon in order to protect country' own information space and own position in the global space becomes especially relevant.

Modern Hybrid Warfare: Russian Federation vs Ukraine

The revolution 4.0 has changed the meaning of both national and international security. It affects the type of conflicts and their nature. A retrospective of military affairs and national security is a history of technological progress. Modern interstate conflicts are increasingly "hybrid"; they combine direct action on the battlefield with non-state phenomena and elements. The line between war and peace, soldier and civilian and even violence and non-violence is blurred [24]. Society information security is an unhindered implementation by society and its individual members of their constitutional rights related to the possibility of free possession, creation, and dissemination of information, as well as the degree of their protection from destructive information. Information policy is designed to promote information security as much as possible, namely the state activities and citizens in the field of production, dissemination, exchange, protection of information, its use in management processes. The greatest threat to today's information security in Ukraine is the hybrid war of the russian federation that is the war combining fundamentally different types and methods of conduct by ignoring the universal values and principles of modern warfare to achieve its goals.

Hybrid warfare is the result of hybrid dangers or threats created by the enemy with the intention and ability to use both traditional and non-traditional means of struggle and influence, depending on the urgent need to achieve enemy goals (according to the NATO Strategic Concept 2010). This is a concentrated, fully controlled and aimed at undermining and destabilizing the opponent, supporting guerrilla movements, covert invasion through the use of various (not necessarily limited to one form) open and secret tactics implemented by coercive military and non-military means (propaganda, disinformation, disinformation, disruption of communications, electricity supply, sabotage, etc.), due to information and economic pressure, the ultimate goal of which is not only to achieve full political influence, but also complete domination over the object - the victim country [3]. We see hybrid threats as a combination of coercive and subversive activities of traditional and non-traditional methods (diplomatic, military, economic, technological) that can be used in a coordinated manner by states or non-state actors to achieve specific goals, remaining below the threshold of formally declared war.

The "ancestor" of hybrid warfare, as well as modern hybrid threats, is the russian federation, especially regarding its illegal actions against Ukraine, as well as modernized ISIS operations that use a huge number of hybrid methods and means against a weakened state. Types and areas of hybrid threats are the following: terrorism, propaganda, organized crime, cybersecurity, piracy, resource scarcity, space, intelligence networks, political movements, speculation and manipulation of historical facts, legal wars, incitement to ethnic and ethnic conflicts. Today, hybrid threats are an effective and efficient tool for russia to change the current world order by regional and global leaders, which causes the significant pressure in the international arena [9].

The fact of Russia' use iWar methods (Hybrid war – does) is confirmed by the following factors: an atmosphere of negative attitude to culture and historical heritage in Ukrainian society is formed; public opinion and political orientation of the Ukraine population are being manipulated in order to create a state of political tension; destabilization of political relations between parties, associations and movements in order to incite conflicts, stimulate mistrust, suspicion, aggravate hostilities, struggle for power; provocation of social, political, national-ethnic and religious clashes; provocation, repressive actions by the authorities against the opposition; reducing the level of information support of government and administration; misleading the population about the work of state authorities, undermining their authority, discrediting their actions; undermining the international prestige of the country, its cooperation with other states; creation or strengthening of opposition groups or movements; discrediting the facts of the historical and national identity of the people; formation of preconditions for economic, spiritual, or military defeat, loss of

will to fight and win; undermining the morale of the population, reducing the country's defense capabilities and combat potential; causing damage to information and technical infrastructure.

According to Polish researcher O. Vasiuta, the “red thread” of the russian hydride war in Ukraine is the ideology of the “Russian World”, which uses various tools to implement its ideology from creating influence in neighboring countries to limiting their sovereignty and establishing full control over their economic, political, informational, religious structures and historical, cultural, and linguistic policies. This is soft power, a form of gradual elimination of state independence. To achieve its goals, the Kremlin uses its attachment to energy resources, buys strategic objects of the chosen state, and seizes the main political levers of the state object of the “russian World”. In addition, there is an extensive promotion of common benefits, and the fifth column is also used. “russian World” encourages constant instability within the chosen state, because on religious and ethnic grounds it calls for the fight against “inorodtsy/resident aliens” (people of other nationalities who are not members of the “russian World”), among whom there is the search for all existent troubles reasons, and firstly terrorism roots [28].

The Russian diaspora, cultural and educational foundations and unions are the main tools for implementing such ideology. In addition, it is planned to deepen the legal project of the “russian World”. An active implementation of real political tasks is among the main directions of the concept, in addition to cultural and educational aspects, namely the development of russian diasporas, increasing their influence on public policy of the countries where they live, using russian-speaking societies as a tool to lobby the Kremlin. Such tasks conflict with the national security of other states [30].

We consider the following to be possible measures to prevent and overcome hybrid threats of the russian federation in the Ukrainian information space [29]: improving and raising public awareness of possible current threats, information on the stability of structures, data protection on the Internet, intensification of international cooperation in this field, development of relevant documents/regulations to prevent and respond quickly to such crises, constant and detailed cooperation with the EU and NATO since the hybrid threats are not limited to internal borders but involve cross-border networks or infrastructure. It is necessary to highlight the clear need to develop hybrid thinking, focusing on mental characteristics such as understanding the strategic context, holistic vision and approach to the operation, focusing on potential, covering the natural complexity of the operating environment.

Information Weapons in the Russian-Ukrainian Confrontation

The formation of a single global information space, which is a natural result of the development of world scientific and technical thought and the improvement of computer and information technology, creates the preconditions for the development and use of information weapons. Possession of effective information weapons and means of protection against them is becoming one of the main conditions for ensuring the national security of states in the 21st century.

Information warfare is characterized by information weapons namely a type of weapon, the main elements of which are information, information technology (including information technology impact technologies), information processes and technical means used in information warfare [21]. Information weapons should be understood as a set of organizational and technical influences on information systems, automated and automatic control systems, communication systems and networks, etc., carried out using systems and means of destruction, distortion, disclosure, theft, creation of false information. It is also represented by systems and means of overcoming protection systems, means of restricting or expanding access to information and resources of legitimate users, systems and means of counteracting and disorganizing the work of technical means, computer systems, systems and tools of information systems resource management [7].

The rapid transmission of large amounts of information is becoming a major challenge in the creation of modern control systems, the solution of which is associated with the development of space communications systems and the widespread use of fiber-optic lines. At the same time, such elements of the information infrastructure become the most vulnerable in terms of information offensive operations. Purposeful organization of such situations is a priority in the case of using information weapons in the course of offensive information warfare and achieving information superiority over the enemy. Effective counteraction to such actions of the enemy determines the purpose of defensive information warfare [25]. The main ways and methods of using information weapons of the russian federation against Ukraine are the following: damage to physical elements of information infrastructure (destruction of power grids, interference, use of special programs that stimulate the decommissioning of hardware and biological and chemical means of destruction of the element base); destruction or damage of information, software and technical resources of the enemy, overcoming protection systems, introduction of viruses, software and logic bombs; impact on software and databases of information systems and control systems in order to distort or modify them; threat or commission of terrorist acts in the information space (disclosure and threat of disclosure of confidential information about elements of national information infrastructure, socially significant and military encryption codes, principles of encryption systems, successful experience of information terrorism, etc.); seizure of media channels in order to spread misinformation, rumors, demonstrate power and bring demands to light; destruction and suppression of communication lines, artificial overload of switching nodes; influence on operators of information and telecommunication systems with the use of multimedia and software tools for subconscious information or deterioration of human health; impact on computer equipment of military equipment and weapons in order to disable them [5].

Use of Chatbots in the Russian-Ukrainian War

Chatbots are computer programs developed on the basis of neural networks and machine learning technologies that communicate using auditory or textual methods. They have become a help to solve the problem of information hygiene and security during the 2022 Russian-Ukrainian war. The Ukrainian Virtual Army is our superiority over an enemy who has nothing like it. russia is launching a million bots that spread messages on social networks, but cannot mobilize a million living people who will sincerely tell the world what they really see, experience, and feel. The information army has three important fronts:

-Global / Western. It is aimed to bring to the world the news of russia's attack on Ukraine, to voice Ukraine's needs and requests for help, to call for tougher sanctions and international isolation of the aggressor. In the first weeks of the war, Ukraine was already on the front pages of all publications and in the first stories of all news releases, but, unfortunately, over time, the world's attention will weaken. Letters, messages, and signatures on petitions will then be needed to hold such attention. Many resources have already been created for this, for example, We Are Ukraine, and multilingual Post to Stop War in Ukraine, Stop Russi Channel|MRIYA, UA Student Union.

-russian. It breaks the plans of the russian government, according to which society should exist in a fictional reality created by the Kremlin propaganda. Such front brings many disappointments to Ukrainians, as Russians are often hopeless.

-Ukrainian. It disseminates important and truthful information, I aimed at helping the government, the military and volunteers to work and coordinate, raises morale and quenchs panic. In a situation of constant stress, danger, uncertainty, healthy communication is helpful and necessary for people [8].

The “information army” that helps the regular army in cyberspace has also defended Ukraine against russia. Activists have created Telegram-bots, where one can “surrender” the enemy as well as volunteer or seek help with housing, medicine,

transport. The Ministry of Digital Transformation has compiled a list of useful chatbots during the war [2].

Bots where one can learn how to join the territorial defense, how to survive a civilian and what to do in a crisis situation are Dzhhut 2.0. Persha dopomoga /First aid/ explains what to do if one does not know or has forgotten the algorithms for emergency help in case of heart attack, stroke, cardiac arrest, and gives other advice on first aid. SaveUA is a bot to help in finding volunteers in specific area or vice versa give the opportunity to offer own help. On March 1, the State Emergency Service of Ukraine launched an information chatbot in WhatsApp with important updates, reliable information, and instructions on emergency response procedures. The Institute of Cognitive Modeling together with the Department of Medical Psychology, Psychosomatic Medicine and Psychotherapy and specialists of the project "Friend" launched a telegram-bot of first aid "Friend. First aid" (@friend_first_aid_bot). The Institute of Cognitive Modeling, the Ministry of Health and the Office of the President of Ukraine have designed a 24-hour psychological assistance platform "Tell me". We are going the same way is the bot to help Ukrainians with cars and people who have nothing to go, find each other. Shelters for Ukrainians is the bot to help people in need of asylum to find those who can provide it.

The Ministry of Digital Transformation and Corezoid have launched a Telegram and Viber for migrants, military and territorial defense chatbot "Turbotnyk". It helps the Ukrainian migrants day and night to get a temporary home and necessary things in CNAPs that work as points of concern.

Many chatbots have been created to gather objective information and evidence of war crimes. Thus, Cyberpolice has launched the following services: a chatbot "Narodnyy mesnyk" in telegram (@ukraine_avanger_bot) where Ukrainians will be able to send information about enemy signs on the country's roads and the movement of Russian aggression forces; SBU chatbot "TRIBUNAL.UA" to collect photo and video evidence for legal claims. Today, every Ukrainian is a witness to the war. All cases of crime must be recorded and used in the legal field in the international arena in order to see vladimir putin in The Hague. The following are recorded: 1. Evidence of murder and violence of civilians or military personnel (murder, torture (beating, rape, mutilation)), hostage-taking or captivity; 2. Evidence of use of weapons and military equipment of the russian federation, shelling, small arms, artillery or air, use of firearms, movement and use of military equipment; 3. Evidence of robbery, seizure and destruction of civil and state property (appropriation and destruction of property, transport, fuel, destruction of cultural monuments); 4. Personal data of the enemy (personal data, documents , passports, call signs and pseudonyms, identification marks). All submitted materials will be collected and used in the case against Russia [11].

The Armed Forces of Ukraine chatbot "eVorog" is a one where Ukrainians can report the movement of the occupiers, enemy equipment and explosive devices for their demining. The service works even without the Internet, and all information is automatically sent to the official chatbot. The main advantage is authorization through Diya. As a result, saboteurs cannot spam fake photos or videos, and the military receives truthful information [2]. Later the official bot "eVorog" launched a new feature that can be used to report the killers in Bucha, Irpen and Gostomel. SBU chat bot "STOPRussianWar" enables to report the movement of enemy equipment, Russian sabotage and reconnaissance groups, troops and equipment of the russian federation; it also has features that can be used to report detected explosive devices and equipment left by the russian occupiers. On March 10, 2022, the SBU expanded the channels for obtaining information from citizens about the war crimes of the Russian occupiers in Ukraine. From now telephone hotlines, emails and other messengers have been added to the Telegram chatbot. SBU has also launched a service "Bachu.info", which can be used to report the movement of russian troops and equipment, even in the absence of the Internet [26].

StopRussia | MRIYA (https://t.me/stopdrugsbot) enables the citizens to send links to enemy channels, groups, and profiles on social networks and messengers such as Telegram, YouTube, Facebook groups, Instagram profiles, which spread misinformation, as well as "leak" the locations of the Armed Forces. To block sabotage resources, one can use the channel https://t.me/stoprussiachannel with the detailed instructions on how to do it. Foundation "Povernys'zhyvym" and volunteers have launched another service - FindOkupant. Znaydy zradnyka! (t.me/Traitor_Search_bot) to collect data on the movement of the Russian military as wells as to inform about traitors and collaborators who collaborated with the occupiers, and to expose Internet agents who "leak" important information to the enemy or distribute content on social networks in support of the invaders. Stop maroder (t.me/stop_marauder_ua_bot) is a chatbot to collect information about looters who steal other people's property during the war. This data will be verified and posted on the SBU website: stopmarauder.com.ua. The civil network Opora has launched a collection of evidence of Russia's war crimes to be presented to the international prosecutor in the Hague. IT company KitSoft has launched a telegram bot SmartNews, which collects news from official sources and they can be filtered by keywords. The State Environmental Inspectorate has created a bot and the website of the Operational Headquarters – Shtab.gov.ua, where one can report environmental crimes in Russia. TacticMedAid, a home care application, has been launched in Ukraine. The Center for Strategic Communications and Information Security at the Ministry of Culture and Information Policy has launched a bot in Telegram and Viber. The Dovidka Info bot gives advice on how to prepare and how to act in emergencies.

The last three months are marked by the following important events: an official chatbot eVorog was launched to enable every Ukrainian to report the location and movement of enemy equipment. More than 10 thousand Starlinks arrived in Ukraine to maintain and restore critical infrastructure. The first IT army was created in the world, which unites more than 300 thousand volunteers who are working to strengthen the country's cybersecurity. A crypto fund was launched and it raised more than $60 million in the crypt to help the Ukrainian army. Artificial intelligence is used to recognize the faces of dead Russians and designed UNITED24 - as the main window for collecting donations in support of Ukraine.

The number of chatbots of the authorities and structures operating on the protection of the information front testifies to the considerable support from the population and the coordination of the institutions actions to protect the information space. Such actions maximally achieve the goals of information hygiene during the war. It involves the ability to think critically, analyze texts and be able to create them. It is also necessary to understand the nature of information and techniques of its impact on the environment and people.

4 Conclusion

Modern globalization processes have qualitatively changed the content and forms of information wars. At the present stage of historical development, the tendency to resolve foreign policy conflicts without armed violence dominates. The information war has ceased to be a secondary factor, a supplement to the "main" events. It has become one of the most important mechanisms of warfare, which is talked about along with the use of armed forces and equipment. All types of hybrid warfare have become a legitimate means of political struggle. Despite the fact that a large part of society is aware of the process of targeted information attack on the enemy and allows the possibility of using "dirty" technologies, it is still subject to manipulation by the media. As a result, the winner in the communicative confrontation is not the one who tells the truth, but the one who managed to show the audience a more exciting "information series" and justify position very clearly. That is, the greater the information and technical capabilities of the country, the more likely the possibility of achieving strategic advantages in the future system of international relations. Hybrid wars have

become an axiom of modern international relations and make it possible to achieve the desired goals quite effectively, with the involvement of small financial and human resources: it all depends on the degree of professionalism of the implementers of information operations. It will be easier for those countries that will have a harmoniously developed and, therefore, protected information society to defend their positions in the information conflict.

Thus, at the present stage, hybrid wars have become one of the main threats to international security, which in the future may lead to the destruction of international relations as such. Uncontrolled information flows pose even greater risks to information conflict.

Literature:

1. "Asymmetric" or "hybrid" war? (On new meanings in the concepts of the postmodern era). http://stratcom.co.ua/asimetrichna-abo-gibridna-vijna-shhodo-novih-zmistiv-u-kontseptah-epohi-postmodernu/
2. Barsukova, O. (2022, April 7). The killer bot "eVorog" can now report on the killers in Bucha, Irpen and Gostomel. *Ukrainian Pravda. Life*. https://life.pravda.com.ua/society/2022/04/7/248140/.
3. Cederberg, A., & Eronen, P. (2015, September 9). How can Societies Be Defended against Hybrid Threats? *Strategic security Analysis*. http://www.defenddemocracy.org/content/uploads/documents/GCSP_Strategic_Security_Analysis_How_can_Societies_be_Defended_against_Hybrid_Threats.pdf/
4. Doroshkevych, A.S. (2015). Hybrid war in the information society. Bulletin of the National University "Law Academy of Ukraine. Yaroslav the Wise". *Series: Philosophy, Philosophy of Law, Political Science, Sociology, 2*, 21–28.
5. Furashev, V.M. (2013). Information security: indicators. *Information and Law, 1*(17), 149.
6. Glossary: educational encyclopedic dictionary on information security. Edited by A.M. Shuliak.
7. Horbenko, I.D., Dolhov, V.I., & Hrinenko, T.O. (1998). Information war - the essence, methods and means of conducting, Legal, regulatory and metrological support of the information protection system in Ukraine, pp. 11–15.
8. How to be a soldier of the information army. 09.03.2022 p. ZAXID.NET; https://zaxid.net/yak_buti_soldatom_informatsiynogo_viyska_n1537918
9. *Hybrid War – A New Security Challenge for Europe*. http://www.parleu2015.lv/files/cfsp-csdp/wg3-hybrid-war-background-notes-en.pdf
10. *Hybrid war – does it even exist?* https://www.nato.int/docu/review/2015/also-in-2015/hybrid-modern-future-warfare-russia-ukraine/en/index.htm
11. Kalatur, A.V. (2022, March 1). Ukraine has set up a chatbot to gather evidence of lawsuits against Putin. *PRAVDA.COM.UA*. https://www.pravda.com.ua/news/2022/03/1/7327053/
12. Karpchuk, N. (2019). Asymmetric war. Glossary: educational encyclopedic dictionary on information security, pp.12-15.
13. Karpchuk, N. (2021). The russian federation propaganda narrative. *Toruńskie Studia Międzynarodowe, 1*(14), 19-30, doi.org/10.12775/TIS.2021.002
14. Kurban O. (2016). *Modern hybrid war: new forms of aggression*. http://ua.racurs.ua/1063-suchasna-gibrydna-viyna-ta-yiyi-vidobrajennya-u-virtualniy-realnosti-chastyna-2
15. Leśnikowski, W. (2016). *Drony. Bezzałogowe aparaty latające od starożytności do współczesności*. Wydawnictwo Adam Marszałek, Toruń.
16. Lind, W.S. (2004). *Understanding Fourth Generation War*. http://www.au.af.mil/au/awc/awcgate/milreview/lind.pdf
17. Luts V. (2015). *Mediawine (media opposition) latest political vocabulary (neologisms, occasionalisms and other innovations).* Lviv: New World-2000, p. 214–215.
18. Marunchenko, O.P. (2013). *Information war in modern political space*. Odesa: Mechnikov University.
19. Marunenko, O. (2011). External and internal information wars in the media space of Ukraine. Education of the region. *Political Science, Psychology, Communications, 4.* 92.
20. Parvar Hamid Ziaei (2004). Soft War (2): Media War. *Tehran International Studies & Research Institute* (TISRI). https://www.fidh.org/IMG/pdf/iran749aweb.pdf
21. Petryk, V. (2009). The essence of information security of the state, society and the individual, Legal Journal, 8, 122-135; www.justinian. com.ua/article.php.
22. Pocheptsov, G. (2017). *The war of the fourth generation is a war of cultures.* https://www.ar25.org/article/viyna-chetvertogo-pokolinnya-ce-viyna-kultur.html
23. Przemysł zbrojeniowy. Tendencje, perspektywy, uwarunkowania, innowacje (2016). Wydawnictwo Uniwersytetu Pedagogicznego, Kraków, pp. 93-118.
24. Schwab, K. (2016). The Fourth Industrial Revolution: what it means, how to respond. *World Economic Forum.* https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond
25. Senchenko, M. (2011). Invisible information wars of the new generation: The theory of network-centric warfare in practice. *Bulletin of the Book Chamber, 11*, 5.
26. SSU has updated the bot "Stop Russian War": you can report explosives and abandoned Russian equipment (2022, April 15). https://ms.detector.media/trendi/post/29347/2022-04-15-sbu-onovyla-bot-stop-russian-war-mozhna-povidomlyaty-pro-vybukhivku-ta-pokynutu-rosiysku-tekhniku/
27. Sudhir, M. R. (2008). Asymmetric War: A Conceptual Understanding. *Centre for Land Warfare Studies Journal, Summer*, 58–66. https://archive.claws.in/images/journals_doc/742067376_MBSushir.pdf
28. Vasiuta, O. (2019). "Russian world" as a technology of penetration / influence of the state. In: A.M. Shuliak (Ed). *Glossary: educational encyclopedic dictionary on information security*, p.426-435.
29. Vozniuk, Ye.V. (2019). *Hybrid threats*. In: Glossary: educational encyclopedic dictionary on information security, pp. 54–56.
30. Wasiuta, O., & Wasiuta, S. (2020). Kremlowska dezinformacja w Internecie i reakcja społeczeństw zachodnich, *Przegląd Geopolityczny, 34*, 136-147
31. Yasiukov, M. (2012–2013). The concept of asymmetric wars as one of the promising approaches to the analysis of wars of the 21st century. *Military-Philosophical Bulletin, 6-7,* 142–150.

Primary Paper Section: K

Secondary Paper Section: JY, KA