DOI: https://doi.org/10.34069/AI/2022.52.04.29
How to Cite:
Ablazov, I., Demenko, O., Leonov, O., Mokliak, S., & Khamula, S. (2022). Information weapons within the interstate struggle in the XXI Century. *Amazonia Investiga*, *11*(52), 269-277. https://doi.org/10.34069/AI/2022.52.04.29

Information weapons within the interstate struggle in the XXI Century

Інформаційна зброя у міждержавній боротьбі XXI століття

Received: April 3, 2022 Accepted: May 5, 2022

Written by:
Ivan Ablazov[123]
https://orcid.org/0000-0001-6293-8043
Oleksandr Demenko[124]
https://orcid.org/0000-0002-1144-0576
Oleksandr Leonov[125]
https://orcid.org/0000-0003-1759-3845
Sergii Mokliak[126]
https://orcid.org/0000-0002-5255-8941
Serhii Khamula[127]
https://orcid.org/0000-0002-0825-7674

Abstract

In particular, information weapons and social media weapons have become a weighty and decisive factor in warfare. Moreover, military conflict models increasingly use information as a weapon in virtual space. The article aims to analyze the peculiarities of the use of information weapons in interstate struggle on the example of empirical assessment of the use of disinformation methods against Ukraine in 2021-2022. Methodology. The study used the methods of cases and content analysis of reports and analytical bulletins of the Centre for Counteracting Disinformation of Ukraine to assess the use of information weapons, in particular the spread of disinformation in the information space of Ukraine. The reports and analytical bulletins from December 3, 2021, to February 21, 2022, were used for content analysis. Results. The main types of misinformation that are spread in the Ukrainian information space are: 1) misleading a particular person or group of people (even an entire nation); 2) manipulation, and 3) creation of the desired public opinion.

Анотація

Інформаційна зброя, зброя соціальних медіа зокрема, стала вагомим та вирішальним фактором у веденні війни. У моделях військових конфліктів все більше використовують інформацію як зброю у віртуальному просторі. Мета статті полягає в аналізі особливостей використання інформаційної зброї у міждержавній боротьбі на прикладі емпіричної оцінки застосування методів дезінформації проти України у період 2021-2022 років. Методологія. У дослідженні використано методику кейсів та контент-аналіз звітів, аналітичних бюлетенів Центру протидії дезінформації України для оцінки використання інформаційної зброї, зокрема поширення дезінформації в інформаційному просторі України. Для проведення контент-аналізу використано Звіти та аналітичні бюлетені за період 3 грудня 2021 року – 21 лютого 2022 року. Результати. Основними видами дезінформації, яка поширюється в українському інформаційному просторі, є: 1) введення в оману конкретної особи, або групи людей (навіть цілої нації);

[123] Professor, candidate of political sciences, associate professor, Professional Development Training Center, Diplomatic Academy of Ukraine named after Hennadii Udovenko, Ukraine.
[124] Scientific secretary, candidate of political sciences, associate professor, State Institution "Institute of World History of the National Academy of Sciences of Ukraine"
[125] Senior lecturer, Law Institute, Department of Political Technology, Kyiv National Economic University named after Vadym Hetman, Ukraine.
[126] Professor, doctor of political sciences, professor, Information Resources Center, Diplomatic Academy of Ukraine named after Hennadii Udovenko, Ukraine.
[127] Professor, candidate of technical sciences, associate professor, Institute of Special Communications and Information Protection, Special Department, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Ukraine.

We determined the main characteristics of fake news (unknown source, manipulative headline, emotional coloring, lack of reference to the head, value judgments). Based on the analysis, trends in the dissemination of false, manipulative information are identified.

Keywords: information weapons, information warfare, hybrid warfare, cyberattack, political warfare.

2) маніпулювання; 3) створення потрібної громадської думки.
Визначено основні ознаки фейкових новин (невідоме джерело, маніпулятивний заголовок, емоційне забарвлення, відсутність посилання на джерело, оціночні судження). На основі аналізу виявлено тенденції у поширенні неправдивої, маніпулятивної інформації.

Ключові слова: інформаційна зброя, інформаційна війна, гібридна війна, політична війна, кібератака.

Introduction

The development of information technology has led to the transformation of information into a certain kind of weapon, allowing potential military action in almost any arena of military action and, most importantly, without military force. Consequently, the concept of information warfare, which actively combines propaganda and cyberattacks to change the global political order, is taking shape. This concept is a paradigm of political warfare, which involves using all the resources of a nation to achieve its goals without the use of armed force.

"Information is now a species of weapon" actively used in military operations before, during, and after conducting them (Jaitner & Geers, 2015). «Information can disorganize governance, delude adversaries and reduce an opponent's will to resist» (Jaitner & Geers, 2015).

In particular, information weapons and social media weapons have become a weighty and decisive factor in warfare. Many countries are trying to build social media influence operations similar to the information war against the United States in the 2016 presidential election (Prier, 2017). It is information that shapes the popularity of the narrative demanded by disinformation developers, fake news. Military conflict models increasingly use information as a weapon in virtual space, which leads to misinterpretation of political events and situations and is used to manipulate consciousness, and control the behavior of information users (Beard, 2014).

The article aims to analyze the peculiarities of the use of information weapons in the interstate struggle on the example of empirical assessment of the use of disinformation methods against Ukraine in 2021-2022.

Literature review

A weapon is defined as a tool used or intended to be used to threaten or cause physical, functional, or mental harm to structures, systems, or living things (Rid & McBurney, 2012). The psychological dimension is a crucial element in using any weapon, occurring in two ways. The first psychological dimension is the intent of the perpetrator to threaten possible harm or to cause damage to an object. The second psychological dimension presupposes that the weapon is used as a threat, declared or assumed to be used: the perception of the weapon's potential does cause psychological harm. It is important to note that an attacker may use a weapon as a threat that can achieve a goal without actually causing physical damage, or an attacker may use a weapon to cause instant damage without threatening to do it first (Rid & McBurney, 2012). Informational weapons use messages to control or manipulate the mind, the perception of the recipient of the weapon (Darraj, Sample & Cowley, 2017; Herrmann, Reserve & Steed, 2018). Fake news spreads in virtual space - an emotional weapon, not concerning private cases or stories, but rather a strategic effort to reduce the level of audience attention from the ongoing debate to manipulate audience feelings, undermining any potential for collective action. Fake news threatens the democratic process in various ways aimed at an outcome contrary to the people's freedom (Loveless, 2020).

Information weapons (IWes) are seen as information-related technologies used in high-precision and intelligence weapons. In other cases, IWes are presented as social media manipulation and propaganda weapons (Thomas, 2020a). Social media is a tool of modern warfare in the information age to spread propaganda by using a narrative and amplifying it through a network of automatically created accounts to popularize that narrative (social media, propaganda, and news and information sharing)

(Prier, 2017). Western countries rarely consider information as a weapon, not separating the term into information-technical and information-psychological aspects. The information technology aspect of IWes includes technologies widely used by many countries for global positioning, intelligence, and electronic warfare on a worldwide scale (Thomas, 2020a). The informational-psychological aspect refers not only to the country's use of information as an online weapon in socio-political arenas but also to the use of disinformation, fake news, the involvement of non-governmental organizations in spreading disinformation, which means creating a "necessary objective" reality and distorting the truth (Selvage, 2021). The informational and psychological aspect of IWes is aimed at covering events in a particular country in the proper context to conduct "political warfare. In the Soviet Union, related terms for IWes were "aid programs" or "aid operations," i.e., tactics designed to change the policy or position of a foreign government in such a way as to "help" the Soviet position (Thomas, 2020a).

IWes are seen as a strategic weapon by the former Soviet Union because of its ability to reach out widely across distant continents (thus, IWes is a planetary weapon). According to a new generation of military experts, IWes have transitioned from "the sphere of quantitative forces to the quantitative-intellectual sphere possible" (Kipp, 2014). Countries form "strategic non-nuclear forces" widely used in next-generation hybrid warfare and will then take on the function of deterrence" (Kipp, 2011).

Information warfare includes cyber strikes and information operations, becoming strategic and considered adequate because of its ability to avoid attribution, contain the reactions of different actors, and minimize costs. However, these components of information wars are asymmetric because they do not allow the victim to defend their positions (Blank, 2017) equally.

The classification of types of IWes depends on information technology. Developers propose acoustic, electromagnetic, radiation, ray, and thermal weapons (Thomas, 2020a), providing "unity of intelligence collection and destruction," namely reconnaissance-fire and reconnaissance-strike systems. Scientists see the development of space constellations as a critical shift in the transition from ground forces to information and aerospace-based details. Intelligence gathering satellites from space provides information that "will form the basis for planning massive, high-precision strikes in a strategic air-space-sea strike operation" (Thomas, 2020a). This idea coincides with the concept of Strategic Operations to Destroy Critically Important Targets (SODCIT), as actively discussed in scientific and expert circles.

In 2010, the changes in the nature of warfare that can manifest in different forms of armed forces and the practical development of SODCIT were noted (Li, Liu, Li & Gao, 2020). Experts indicated that it is appropriate to combine strategic defensive, offensive, and ocean warfare operations into a single strategic process (Bae & Park, 2019). IWes and its broad coverage of strategic targets through space-based systems will be crucial in such operations. Consequently, supporting a strategic operation to destroy critical enemy targets requires the use of space-based intelligence assets for these targets: electronic intelligence assets; meteorological intelligence assets for proper selection of combat assets and modes of engagement; and space-based navigation, communications, relaying, and strike assessment systems (Van Vuuren, 2018).

The literature notes that IWes and its assets are built on information technology. Thus, the concept of SODCIT refers to the extensive use of IWes as non-nuclear strategic weapons or assets. Such use in combination with high-precision munitions or air-space forces is significant because it enables long-range access to enemy territory anywhere on the globe. Over the past two decades (2000-2020), experts and academics have discussed the development of the IWes concept, which includes new developments in information technology and the emergence of new ways of using information technology and information-psychological applications of IWes.

ICT supports warfare in two ways: providing new weapons for deployment on the battlefield, such as drones and semi-autonomous operations, which are used to engage ground targets, disarm bombs, and patrol, and providing what is known as information advantage, the ability to collect, process and disseminate information. The information advantage is also a result of the use of ICT, exploiting or denying the adversary's ability to do the same. ICT is proving to be an effective and profitable military technology because it is efficient and relatively cheap compared to the overall costs of traditional warfare (Arquilla & Borer 2007; Steinhoff, 2007). For this reason, the use of ICT in warfare has snowballed since the 2000s. This year has defined some profound changes in the way war is conducted. ICT has started the latest revolution in warfare by providing new tools and processes of war such as network-centric warfare (NCW), integrated command, control, communications, computers, intelligence, surveillance, and reconnaissance (Taddeo, 2012).

Research on information weapons began in the 1990s, defined as a specially selected piece of information capable of causing changes in the information processes of information systems (physical, biological, social, etc.) per the actor's intentions who is using the weapon. Information weapons are used to destroy, distort, or steal data files; to copy or retrieve desired information from those files after penetrating security/firewalls; to restrict or prevent access to data by authorized users; to introduce disruption or disorder to technical equipment (Thomas, 2020a).

One form of information weapon is propaganda and disinformation, which can change the information component of control systems, creating a virtual picture to change reality, the human values system, and manipulate the moral and psychological life of the enemy's population. This type of weapon can create disinformation in protected systems and alter navigational systems, information and weather monitoring systems, precision time systems, etc. (Thomas, 2020b).

Thus, the literature is actively studying the problem of information weapons in the context of the concept of information political warfare as a resource to achieve the goals of an individual nation without direct military invasion.

Methodology

The study used the case methodology and content analysis of reports, analytical bulletins of the Centre for Counteracting Disinformation of Ukraine to assess the use of information weapons, in particular, the spread of disinformation in the information space of Ukraine by the following methods:

1. Biased presentation of facts;
2. Disinformation from the opposite direction;
3. Terminological "mining."

The reports and analytical bulletins for December 3, 2021, to February 21, 2022, were used to conduct the content analysis.

Results

The Center to Counteract Disinformation (hereinafter referred to as the Center) is a working body of the National Security and Defense Council of Ukraine, established per the decision of the National Security and Defense Council of Ukraine dated March 11, 2021 "On Creation of Counteracting Disinformation Center," enacted by the Decree of President of Ukraine dated March 19, 2021 No. 106. The Center ensures the implementation of measures to counteract current and projected threats to national security and national interests of Ukraine in the information sphere, ensure information security of Ukraine, identify and counteract disinformation, effectively counter-propaganda, destructive information influences, and campaigns, prevent manipulation attempts. The activity highlights the tendencies of informing about the state of military affairs, defense industry, fight against crime and corruption, foreign and domestic policy, economy, critical infrastructure facilities, environment, health, social sphere, formation of public consciousness, scientific and technological direction and so on. The main focus is on countering the spread of false information and combating information terrorism.

The Center is actively involved in fighting Russian aggression, and its priorities are operative informing the population, revealing misinformation and manipulation, ensuring information security, and combating information terrorism.

Disinformation (French des - denial and information) is a deliberately false, twisted message disseminated to mislead the public and politicians. It is also used to weaken opponents' positions, hide their miscalculations and defeats, and regroup. Often it becomes the primary weapon to achieve political, military, propaganda, and other goals.

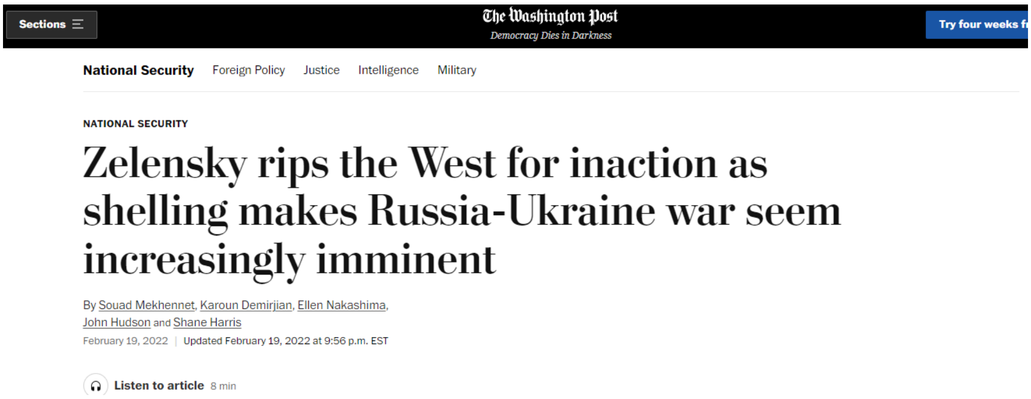
The main types of disinformation spread in the Ukrainian information space are:

1) misleading a particular person or group of people (even an entire nation);
2) manipulation;
3) creating a desired public opinion.

The main signs of fake news are:

1. Unknown source.
2. Manipulative headline.
3. Emotional tone.
4. Lack of reference to the source.
5. Evaluative judgments.

For example, the analysis of the "Munich Security Conference" topic coverage in the world media shows a generally objective coverage of the facts about the security situation in Ukraine and Europe by the world media (The Washington Post, France 24, The Guardian, Polsat News), the unity of different European countries. Particular attention is paid to the "emotional speech" of the President of Ukraine. However, the information is presented restrainedly with an unbiased assessment of the words. Information resources of the Russian propaganda ecosystem focused on the actions of Ukraine, which were emotionally covered with a manipulative headline, providing subjective evaluative negative judgments about the potential of Ukraine (Newsletter).

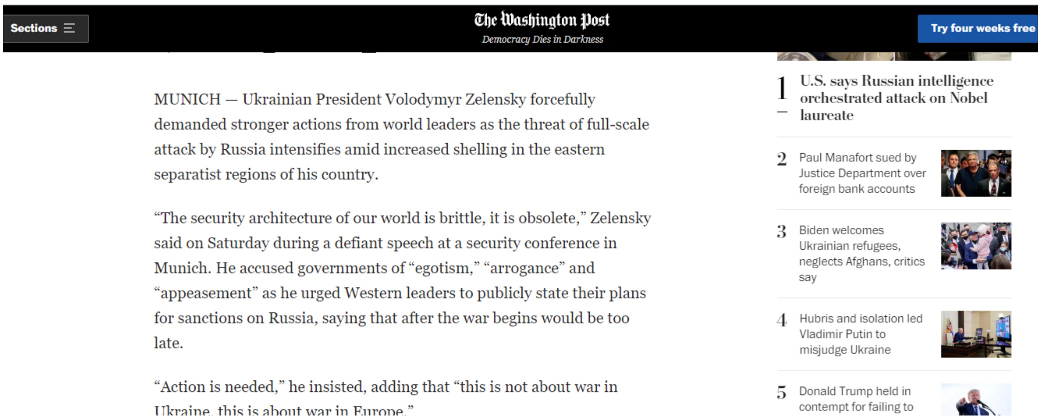


NATIONAL SECURITY

Zelensky rips the West for inaction as shelling makes Russia-Ukraine war seem increasingly imminent

By Souad Mekhennet, Karoun Demirjian, Ellen Nakashima, John Hudson and Shane Harris
February 19, 2022 | Updated February 19, 2022 at 9:56 p.m. EST

a)



MUNICH — Ukrainian President Volodymyr Zelensky forcefully demanded stronger actions from world leaders as the threat of full-scale attack by Russia intensifies amid increased shelling in the eastern separatist regions of his country.

“The security architecture of our world is brittle, it is obsolete,” Zelensky said on Saturday during a defiant speech at a security conference in Munich. He accused governments of “egotism,” “arrogance” and “appeasement” as he urged Western leaders to publicly state their plans for sanctions on Russia, saying that after the war begins would be too late.

“Action is needed,” he insisted, adding that “this is not about war in Ukraine, this is about war in Europe.”

1 U.S. says Russian intelligence orchestrated attack on Nobel laureate

2 Paul Manafort sued by Justice Department over foreign bank accounts

3 Biden welcomes Ukrainian refugees, neglects Afghans, critics say

4 Hubris and isolation led Vladimir Putin to misjudge Ukraine

5 Donald Trump held in contempt for failing to

b)

Figure 1. The Washington Post: Munich Security Conference.
Source: The Washington Post (2022).

Analysis of reports by the Center for Countering Disinformation reveals the following major trends in the dissemination of false, manipulative information:

1. Detailed information campaigns as part of a "military operation," including information threats and disinformation narratives embedded in media news.
2. Dissemination of non-legal information and fakes in several waves and stages in various communication channels: involvement of public persons, automatic creation of accounts in social networks, creation of telegram channels to spread disinformation, accounts in social networks under the guise of various charitable non-profit structures.
3. Implement separate information campaigns aimed at specific target audiences, including the U.S. and EU countries.

Disinformation content aims to destabilize the internal situation in Ukraine and increase panic among the population. The primary purpose of propaganda is to spread the opinion about Ukraine as a terrorist country, promote narratives about the incompetence of the authorities and impossibility of defending its borders, improper fulfillment of its obligations by foreign partners. Inflammation, information manipulation, and the spreading of blatant fakes about the threat of war accompany information policy and campaigns.

During the content analysis of the Center's main messages on propaganda and disinformation in Ukraine, covering fake manipulative news, the following features of information warfare in the virtual information space of Ukraine were identified:

- carrying out dangerous information and psychological operations with different purposes, in particular, aimed at creating the illusion of stabilization of life in the occupied territories;
- conscious manipulation of facts;
- information terrorism and blackmail, using public figures to target Western audiences to spread various narratives and psychological pressure;
- the use of government services to legalize the activities of their propagandists;
- disinformation globally about Ukraine's defeat through multiple communication channels and fake news;
- formation of untruthful terminology;
- biased commentators on social networks posting texts from their handlers to gather information about explosions or infrastructure.

Information terrorism is violent and coordinated influence, filled with disinformation, all kinds of manipulation, and aimed at introducing society into a state of informational terror - permanent oppression, panic, disorientation. The people behind this influence are info-terrorists. To create manipulative content, they not only compose but also commit crimes themselves. Info-terrorists, unlike propagandists, are operators, coordinators, journalists, SMM specialists, etc.

The classification of information weapons of the Center for Counteracting Disinformation

A violent confrontation in the global information space leads to full-fledged information wars. There are many classifications of information wars. We consider three main types: information-psychological wars (IPW), cybernetic wars (CNW), and mixed type information wars (MW) (Kaczynski, 2022).

The latest information technology, current information, and psychological forms and ways of influencing personality and society give rise to many different types of information weapons.

We consider the mental weapon (MNW) as a weapon aimed at changing identity. Under the conditions of modern information wars, ensuring the security of the national cultural space and its protection from mental weapons is of particular importance.

Special Information Operations (SIO) are information weapons that use not only media but also the capabilities of culture and art, as well as psychotropic and psychotronic methods of striking consciousness, and what is more dangerous - substitution of consciousness.

Information weapons aimed at defeating the consciousness include cognitive weapons (CW), which can infect the mass consciousness with cognitive viruses like memes. By infecting the consciousness, "reprogramming" it, meme viruses, like an information virus, spread in the mass consciousness.

Content Weapon (CNW) is a weapon aimed at changing the properties of the human intellect. Its primary tool is the content of the information message, constructed in a particular way and which can be presented in multimedia, text, or graphical format.

Cyber Weapons (CBW) are a weapon that uses computer networks to carry out various politically oriented cyber-attacks. It is used by individual hackers, terrorist groups, and states alike. Viruses such as "logic bombs" and "Trojans" pose a particular threat here.

Information-Algorithmic Weapon (IAW) is a weapon that, using psychophysical methods, affects the human brain through visual images of cyberspace and turns people into conductors of predetermined ideas-algorithms. The purpose of this weapon is to adjust the cultural code.

The core of networked weapons (NW) is a set of actions to shape the intended behavior of both individuals and specific community groups in times of peace, crisis, or war. Networked ways of organizing interactions and implementing collective actions change our communities. It is accomplished through information technology, from the smartphone to the Internet.

Behavioral Weapons (BW) is a non-fatal weapon that aims to change the behavior of individual groups of people or the enemy as a whole. It aims to create special conditions when a person prefers not to make decisions independently but automatically imitate other people's habits, stereotypes, etc. (Kaczynski, 2022).

Discussion

Disinformation is used to destroy trust, undermine morale, degrade the information space, undermine public discourse, and increase commitment to the government of the country by spreading fake news (Lucas & Pomeranzev, 2016). However, the human ability to react is limited due to the limited ability to cover the entire information space and critically analyze the credibility of information. Therefore, understanding the critical attributes of fake news minimizes the destructive impact of propaganda and misinformation. Furthermore, myth-busting and fact-checking are carried out by a limited number of people with developed critical thinking. Therefore, to counter disinformation, an approach that adjusts to different groups of people and target audiences should be used to build trust between polarized groups.

Lucas & Pomeranzev's (2016) recommendations for countering disinformation include tactical, strategic, and long-term priorities focusing on disinformation and media strengthening in democracies and audience education. The main suggestions are:

1) Systematic analysis of the disinformation impact on citizens and their level of trust in government, including selecting tools and instruments of such research to track content and news in different countries, comparing them with each other. Such analysis will provide a holistic understanding of effective responses to propaganda. A detailed analysis of the media environment will identify misinformation campaigns and understand the sources of public awareness. Systematic analysis should include monitoring social media and identifying trends and personalities popular among polarized social groups that can be engaged to build trust.
2) Ensuring media quality by regulating political advertising, correcting media mistakes, and creating effective regulatory institutions. It is advisable to hold consultations of young regulators by the International Commission under the auspices of the Council of Europe, modeled on the Venice Commission, which monitors the observance of the rule of law and democratic standards. It will help to solve this problem.
3) New agencies and new cooperation. The establishment in Ukraine of the Center for Counteracting Disinformation is a practical example of counteracting propaganda. Creating strategic communications departments is also a feasible response (Lucas & Pomeranzev, 2016).
4) Deconstruction of disinformation through investigation of propaganda by international organizations (Global Witness, Transparency International) and destruction of myths for the critical audience, susceptible to arguments based on facts. It is advisable to use technology to automate fact-checking, search for automated chatbots, train media professionals, and develop disinformation ratings.
5) A working group to address the distortion of history and the spread of false syllogisms linking to contemporary events. The working group should include psychologists, historians, sociologists, and media specialists to create an "ideas factory" to develop ways to approach the historical and psychological trauma of victims of historical events (wars, conflicts) and coverage of other narratives of such events.
6) Targeted interaction using social media technology. For example, Facebook technology is used to deradicalize far-right extremists and jihadists.
7) Restoring public speech to define standards of journalism and social and civic issues.
8) Media literacy involves training media consumers to identify misinformation. Pilot projects are operating in Ukraine, particularly IREX, which uses new techniques to expose misinformation outside the academic environment. Media literacy projects should use both online and television media channels.

Blank's (2017) study of Russian cyber warfare and information warfare strategies and practices in Estonia, Georgia, and Ukraine between 2006 and 2016 demonstrates the close connection between cyberattacks and disinformation, which provided effective planning and power projection capabilities. Propaganda operations by specialized computer network offices preceded cyber-attacks. Such practices are consistent with the concept of political warfare and information operations, where cyber warfare is identical to information operations. This practice is characterized by the attributes of information confrontation or information warfare and is integrated into any military operation campaign. The concept of information warfare has been used since the conflict in Chechnya in 1999-2000, clashes in Estonia, Georgia, and Ukraine, corresponding to the political warfare paradigm. Information weapons and operations are a means of information warfare, a defining feature of being used to fight insurgencies internally

(Blank, 2013). Political warfare, in turn, is a logical application of Clausewitz's doctrine in peacetime. Broadly defined, political warfare uses all means of a nation, except war, to achieve its national goals (Pomeranzev, 2015). Such operations are conducted overtly and covertly; varying from overt actions such as political alliances, economic measures (like ERP - European Recovery Plan - Marshall Plan), "white" propaganda, covert operations such as covert support for "friendly" foreign elements, "black" psychological warfare, and even encouraging underground resistance in hostile states (Blank, 2017).

Consequently, according to Microsoft, Russian-linked hackers began conducting cyberattacks against Ukraine a year before the Russian military invaded in 2022 to lay the groundwork for future military operations. Between February 23 and April 8, 2022, Microsoft recorded 37 devastating cyberattacks against Ukraine by Russian hackers. 32% of the hacker attacks were directed against Ukrainian authorities, while more than 40% were directed against organizations in critical sectors of the economy. The Microsoft Threat Intelligence Center (MSTIC) detected wiper malware on more than a dozen networks in Ukraine and disarmed it. Before Russia invaded Ukraine, MSTIC witnessed 237 cyber-attacks by Russian hackers against Ukraine.

Conclusion

The main types of disinformation spread in the Ukrainian information space are:

1) Misleading a particular person or a group of people (even an entire nation).
2) Manipulation.
3) Creation of the desired public opinion.

The main characteristics of fake news (unknown source, manipulative headline, emotional coloring, lack of reference to the head, value judgments) were determined. Based on the analysis, trends in the dissemination of false, manipulative information are identified. Detailed information campaigns developed as part of a "military operation" include information threats and disinformation narratives. The dissemination of non-legal information and fakes in several waves and stages in various communication channels has been revealed: the involvement of public persons, the automatic creation of accounts in social networks, the creation of telegram channels to spread disinformation, accounts in social networks under the guise of various charitable non-profit structures. In addition, it has been established that there are separate information campaigns aimed at specific target audiences, particularly the U.S. and EU countries. Disinformation content seeks to destabilize the internal situation in Ukraine and increase panic among the population. The information policy and campaigns are accompanied by disinformation, information manipulation, and the dissemination of outright fakes about the threat of war.

Bibliographic references

Arquilla, J., & Borer, D. A. (Eds.). (2007). Information strategy and warfare: A guide to theory and practice. Routledge.

Bae, S. H., & Park, D. W. (2019). Cyber weapon model for the national cybersecurity. Journal of the Korea Institute of Information and Communication Engineering, 23(2), 223-228.

Beard, J. M. (2014). Legal phantoms in cyberspace: The problematic status of information as a weapon and a target under international humanitarian law. Vand. J. Transnat'l L., 47, 67.

Blank, S. (2013). Russian information warfare as domestic counterinsurgency. American Foreign Policy Interests, 35(1), 31-44.

Blank, S. (2017). Cyber war and information war a la russe. Understanding cyber conflict: Fourteen analogies, 1-18. [File PDF]

Darraj, E., Sample, C., & Cowley, J. (2017, June). Information operations: The use of information weapons in the 2016 US presidential election. In Proceedings of the 16th European Conference on Cyber Warfare and Security (pp. 92-101).

Decree of President of Ukraine No. 106. "On the establishment of the Center for countering disinformation" dated March 19, 2021. Available at: https://www.president.gov.ua/documents/1062021-37421.

Herrmann, L. C. J., Reserve, U. A. F., & Steed, L. C. B. (2018). Understanding Information as a Weapon. Military review online exclusive, 1.

Jaitner, M., & Geers, K. (2015). Russian information warfare: Lessons from Ukraine. Cyber war in perspective: Russian aggression against Ukraine, 87-94.

Kaczynski A. (2022) Structural model of organization of information and information-psychological security. CPD. Available at: https://cpd.gov.ua/articles/структурна-модель-організації-забез/ (Tsentr prodii dezinformatsii pry RNBO Ukrainy).

Kipp, J. (2011). Russia's Nuclear Posture and the Threat That Dare Not Speak Its Name. Russian Nuclear Weapons: Past, Present, and Future, JSTOR, 459-503.

Kipp, J. W. (2014). 'Smart Defense' from New Threats: Future War from a Russian Perspective: Back to the Future after the War on Terror. The Journal of Slavic Military Studies, 27(1), 36-62.

Li, O., Liu, B., Li, C., & Gao, D. (2020). Demand Forecast of Weapon Equipment Spare Parts Based on Improved Gray-Markov Model. International Journal of Advanced Network, Monitoring and Controls, 5(3), 47-56.

Loveless, M. (2020). Information and Democracy: Fake news as an emotional weapon. In Democracy and Fake News (pp. 64-76). Routledge.

Lucas, E., & Pomerantsev, P. (2016). Winning the information war. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe. Washington: The Center for European Policy Analysis.

Pomeranzev, P. (2015). Authoritarianism Goes Global (II): The Kremlin's Information War. Journal of Democracy, 26(4), 40-50.

Prier, J. (2017). The command of the trend: Social media as a weapon in the information age. SCHOOL OF ADVANCED AIR AND SPACE STUDIES, AIR UNIVERSITY MAXWELL AFB United States.

Rid, T., & McBurney, P. (2012). Cyber-weapons. the RUSI Journal, 157(1), 6-13.

Selvage, D. (2021). From Helsinki to "Mars" Soviet-Bloc Active Measures and the Struggle over Détente in Europe, 1975–1983. Journal of Cold War Studies, 23(4), 34-94.

Steinhoff, U. (2007). On the ethics of war and terrorism. OUP Oxford.

Taddeo, M. (2012). Information warfare: A philosophical perspective. Philosophy & Technology, 25(1), 105-120.

The Washington Post (2022). Zelensky rips the West for inaction as shelling makes Russia-Ukraine war seem increasingly imminent. Available at: https://www.washingtonpost.com/national-security/2022/02/19/ukraine-russia-munich-zelensky/(Washingtonpost)

Thomas, T. (2020a). Russian Military Art and Advanced Weaponry. The MITRE Corporation.

Thomas, T. L. (2020b). Information Weapons: Russia's Nonnuclear Strategic Weapons of Choice. The Cyber Defense Review. Vol. 5, No. 2, Special Edition: Information Operations/Information Warfare (SUMMER 2020), pp. 125-144. https://www.jstor.org/stable/26923527?seq=1

Van Vuuren, R. (2018). Information Warfare as Future Weapon of Mass-disruption, Africa 2030s Scenarios. Journal of Futures Studies, 23(1), 77-94.