DOI 10.31558/2519-2949.2023.2.11
УДК 304.4:316.7:32

ORCID ID: https://orcid.org/0000-0002-8827-3569
Saschuk H. M., Taras Shevchenko National University of Kyiv

SECURITY IMPERATIVES OF THE UKRAINIAN INFORMATIONAL SPACE IN CONDITIONS OF THE HYBRID WARFARE

The essence of the "hybrid war" is clarified, as a full arsenal of various types of combat operations (bombing of civilian infrastructure, terrorism, disorderly, brutal, unprovoked violence), as well as informational and psychological pressure on citizens of one's own country and on citizens of the country – occupations involving state and non-state actors.

Mechanism of providing informational security of Ukraine is analyzed, it's efficiency as some system of connected by itself parts from the content of which – from the normative and institutional base of the content – to the inter-sectoral interaction of information security subjects, the implementation of a free state course in the information sphere depends.

It has been shown that russian approach to the informational warfare – it is global strategy which includes cyber attacks and also informational operations against most of the democratic actors in the world, that russian campaign of the informational warfare continue to discredit democratic institutions, promoting extremism and discontent, supporting anti-democratic leaders, trying to shake the influence of the West.

Russian information strategies, using a wide range of disinformation tools, "troll factories", etc., were found to be aimed at restoring Russian dominance in the post-Soviet/imperial sphere of influence; reducing the influence of Western democratic values, institutions and systems in order to create a polycentric world model; the expansion of Russia's political, economic and military hegemony throughout the world.

It is grounded, that the hybrid war unleashed by the Russian Federation against Ukraine is not only a challenge to the existence of an independent Ukrainian state, the danger threatens the entire system of international and European security and leads to the destruction of the existing security architecture, discrediting its main structures such as NATO, the EU, the OSCE, the charter of the UN and the Helsinki process regarding the inviolability of borders and state sovereignty.

Keywords: *informational space, informational warfare, hybrid war, propaganda, extremism, terrorism.*

Introduction. In modern conditions information touches all of the life and activity spheres of the man and state, is becoming a direct production resource along with raw materials and energy, one of the wealth of the country, its national property. That's why without the presence of timely and reliable information, the functioning of any type of national security is practically impossible.

Russia's unprovoked, inhumane, war of aggression against Ukraine has been going on since February 2014. The Kremlin lacked the honor and courage to recognize the fact of aggression, so it cowardly hides its own imperial adventures under the mask of hybridity, betting on the support of local collaborators, raids by its armed forces, subversive and subversive activities, aggressive and lying propaganda, where is the image of a Ukrainian in the Russian information space is formed in the form of a "Khohl", a "Banderivite", a "Ukrainian fascist", when the Russian mass media do not utter total lies, resort to classic methods of manipulating the mass consciousness, the task of giving an effective and meaningful response to direct military and information aggression against our country.

Research purpose. To analyze essence of the russian informational strategies and means of their resistance.

Analysis of the last researches. The problem raised in the article was studied by such scientists as O. Batrymenko, O. Bilorus, O. Vlasyuk, V. Horbatenko, V. Horbulin, O. Jus, O. Dubas, O. Zernetska, V. Kolyadenko, Ya. Lyubivy, V. Lyakh, E. Magda, H. Pocheptsov, K. Raida, O. Sosnin, T. Kremen and others.

Presenting main material. Russia used against Ukraine conception of the such called "hybrid" by it's content war, in other words it's connection of the information-psychological influence "with tools

and elements of the different forms of military-political conflict: trade, partisan, sabotage, civil war, military occupation, terrorism involving state and non-state actors. Such connection of different elements and forms of waging war called “hybrid war”. One of the authors of hybrid war conception is F. Hoffman who described them as “ a full arsenal of various types of combat operations, including conventional capabilities, irregular tactics and formations; acts of terrorism, disorderly violence and criminal power” [1, p.17].

Hybrid wars can be waged both by the state and by non-state actors. That is, the state, which unleashes such a mixed war, concludes an agreement with non-state executors – militants, terrorists, separatists, mercenaries, other organizations and groups of the local population, the connection with which is formally denied. They are entrusted with functions that are unacceptable for the state itself in view of the obligation to comply with the provisions of the Geneva and Hague Conventions on the Laws of Land War, as well as agreements with other countries. Therefore, all the "dirty work" can be shifted to the shoulders of non-state formations.

This creates an impression of the "blurring" of the contours of a military conflict and the involvement of non-military means in it, which in their usual state have no direct relation to a classic military confrontation [2].

Usually “hybrid war” called as “hybrid aggression”. Thus, under the term "hybrid aggression" the Ukrainian researcher E. Magda proposes to understand a complex of heterogeneous methods of influence on the enemy, adjustable in size and combined in nature, in which the actual military component is not dominant. Hybrid threat predicts usage by the enemy different combinations: 1) political, military, economical, social, informational tools [3, p. 262-263]. Similar terminology is used by T. Polyoviy and H. Yuskiv. “Russian “hybrid aggression” against Ukraine which was started in the February of the 2014 with the annexation of Crimea and still continues in Donbas, demonstrated wide spectre of methods and tools of influence. During the last years it were published a lot of researches, by both Ukrainian and foreign authors, who examine the goals, mechanisms, and means of influence of the Russian Federation in Ukraine and Europe. Russia uses the information sphere as an integral tool of "hybrid aggression" against Ukraine” [4, p. 86].

Undoubtedly, the modern Ukrainian-Russian war should be considered a hybrid, although the number of human victims and material losses does not decrease from such recognition. Such a war produces suitable "warriors". It is about the "fighters of invisible fronts" that the "great-power" Moscow is trying to open in the Ukrainian rear, seeking to defeat its main opponent in the post-Soviet space with the hands of traitors, since its own hands turned out to be unsuitable for either a plow, a sword, or a pen. Between mentioned “fighters” and crying-politicians (“voices of the apocalypse”) which are causing different troubles for their Motherland, only to get more power or only to be in the centre of attention; and just mercenaries, which are ready to do the dirtiest work for the money; and “useful idiots”, who are sincerely belive in the basic enemy propaganda, spreading its most absurd provisions; and a variety of political adventurers and swindlers trying to make a career out of the hardships of war and profiting from socio-economic woes.

Thus, the propagandistic and financial infusions of the neo-imperial Kremlin formed a social base in Ukraine for waging a hybrid war, which is composed of deeply flawed people, primarily in the moral sense. Carrying out invasive and destructive plans for Ukraine, the Russian Federation chose the worst representatives of Ukrainian society for their implementation – pathological traitors, profiteers, scoundrels and bribe-takers and the rest of the inhabitants of the moral and political "bottom". It is likely that the new Russia – truly democratic, truly free, truly federal, which will inevitably emerge after the "restructuring" of the current Russian Federation – will establish contacts with the best representatives of Ukraine.

The diversity of the Kremlin’s "hybrid warriors" in Ukraine is not so much impressive as it makes us think about shades of cynicism, meanness, and self-interest. There is another category of these pro-Moscow ideological warriors, which is pairwise correlated with the category of "useful idiots" and can be defined as "selfish spotlights." We are talking about "black ideologues", who are somewhat similar to "black archaeologists". They are robbing the treasury of national history – the national historical experience, replacing real values with false and hostile ones and turning this experience into a subject of cynical bargaining with the enemy. In particular, it is already clear today that the idea of "people’s republics", into which the Kremlin’s "hybrid commanders" planned to divide Ukraine, has a Ukrainian origin and was thrown to the Moscow masters by their local ideological servants, who are more or less familiar with the experience of Ukrainian state-building at the beginning of the last century” [5, p. 517-518].

If "the primary task of the Russian hybrid war was an attack on Ukraine, today its informational component – according to O. Vlasyuk – is aimed at Europe. At the same time, the Russian vision of the war

in Ukraine is imposed on the European political community. The latter is presented as a "failed state", that is, a state that did not occur. The opinion is imposed on the European expert environment and mass consciousness that Ukraine is a purely oligarchic entity, it destroys its own citizens and has never been a state" [6, p.21]. The scale of the information war launched by Russia against Ukraine was quite aptly said by the Commander-in-Chief of NATO's combined armed forces in Europe, F. Breedlove: "This is the most amazing information blitzkrit that we have ever seen in the history of information warfare." [7].

According to O. Vlasyuk, today one can see at least two dominant lines along which Russia "hits" EU countries with information in the context of the Ukrainian crisis.

The first goal is to try to reach mutual understanding with the West, primarily by "economizing" the Ukrainian-Russian war. That is, to prove to the West that it does not make sense for it to get involved in a protracted confrontation with Russia, since it hits the pockets of ordinary Europeans. The main task here is to bring the problem from the space of regional and global security to the level of an ordinary "calculator". And it should be noted that the strategy of appealing to the "stomach" can be quite effective.

The second goal is to break the Euro-Atlantic unity, increasing the existing contradictions between Europe and the United States. There is targeted propaganda of the idea that the USA is trying to wage a war (primarily economic) with Moscow with the hands and funds of Europeans, which harms the interests of European capitals. This strategy is also quite successful, and politicians who defend extremely pro-Russian positions come to power in a significant number of countries. Today it is already Greece. Next is France. And with regard to the latter, it is not only about the nationalists of Marie Le Pen, but also about the political power of Nicolas Sarkozy. Russia's position in some Eastern European countries is also strong [8].

The NATO leadership more or less clearly understands the problem of destructive Russian influences. To counter these influences, a step in the right direction was the creation in 2014 of the NATO Center of Excellence for Strategic Communications, whose priority is to study the issues of "hybrid wars," Russian information campaigns, and the Kremlin's destructive propaganda efforts. According to the results of the September (2014) NATO summit in Newport, the issue of strategic communications reached the level of final decisions. Moreover, paragraph 13 of the NATO Summit Concluding Statement clearly establishes the relationship between "hybrid warfare" and "strategic communications".

Unforunatelly, EU is so far yet from such precise organizational self-determination in case of countering Kremlin propaganda and does not fully understand that russian propaganda machine – it's not only "mass media" in their traditional meaning. Paraphrasing the well-known definition of war, given by the Prussian general Karl von Clausewitz, as "the continuation of politics by other means", in relation to the Russian mass media, we can say that they are the means of continuation of the Kremlin's aggressive policy, which, as already mentioned above, has almost completely lost contact with the classical understanding of the media as information "intermediaries" inherent in the democratic world.

It is precisely because of the Kremlin's geopolitical claims that funding for international studios of leading Russian TV channels is increasing year by year, and Russia Today, RT, a foreign policy broadcasting channel created at the end of 2005, already has a budget of hundreds of millions of dollars. In fact, Russia has restored for its own mass media the classic Soviet model of the press, when there was no "truth" in "news" and "news" in "truth". It's just that the place of "Pravda" and "Izvesti" was taken by other electronic publications.

Keeping pace with technological progress, Russia has intensified its activities on the Internet, and especially in social networks. And not only in networks of Russian origin ("Odnoklassniki.RU"; "V Kontakte"), but also in Russian-speaking and foreign-language segments of networks such as "Facebook" and "Twitter". In this regard, some British publications directly warn their readers about the influx of Russian commentators on the websites of electronic versions of their publications and that a tough propaganda war is being waged against publications that condemn Russia's aggressive policy. The heads of the Security Service of Ukraine and other Ukrainian security forces have repeatedly warned about Russian cyber aggression. In an extremely short period of time, Russia created hundreds of artificial accounts of fake users for the purpose of waging an information war in social networks. The recently created "information troops" of Ukraine (initiative of the Ministry of Information Policy) are quite successfully fighting against such "Kremlebots", but it must be frankly admitted that the initiative is not on the side of Ukraine yet. And initiative in war is a good half of success.

It is difficult to oppose Russia's aggressive information policy, if only because Russia invests enormous amounts of money in this activity, which in terms of total volume exceed the funds spent on similar activities by any other countries on the European continent. Russia's advantage is the integrity of information events and campaigns, which is not least helped by the total control of the Russian mass media by the Kremlin.

Hence the possibility to launch messages and carry out special information operations along all "azimuths" at the same time. Ukraine and other democratic European states cannot afford to respond to Russian informational aggression in the same Russian style, so as not to turn into authoritarian "dragons" like Russia [9].

However, all of the above does not mean that Ukraine and democratic Europe will not find an asymmetric democratic response to the threats and challenges of aggressive Kremlin propaganda in the near future. Especially if the EU countries realize that countering the Kremlin's informational aggression is as urgent a priority for them as it is for Ukraine. At the same time, European partners should understand the value of Ukraine as a partner, because during the long-term ideological confrontation with Russian aggression, Ukraine has developed a certain informational immunity, it has obvious strong internal safeguards, which were formed either situationally or forced during the last year of the active struggle for independence and territorial integrity [8].

Infromation frontline of the hybrid war speads, as V. Horbulin rightly observes, at the same time on the different directions. Above all: (1) among the citizens in the area of conflict, (2) among the population of the country against which the aggression is carried out, but whose territory is not covered by the conflict, (3) among the citizens enemy country, in other words against their citizens creating there behavior model which largely obeys the messages of the federal press and (4) among international community, creating "funds", "cultural communities", "analytics centres", using "experts" of prorussian direction in Europe, and also activity of the RT channel [10, p. 9].

The information component has indeed become a cross-cutting theme of hybrid warfare. And in the Ukrainian case, we are dealing not just with enemy propaganda, but with what experts call a "war of meanings", for the retransmission of which the whole set of information delivery channels is involved. The main structural elements in this war are simulacra, i.e., images of something that does not exist in reality, for example: "fascists in Kyiv", "atrocities of punitive battalions", "crucified boys", "use of weapons prohibited by Ukraine", etc. The purpose of exploiting such simulacra is to replace citizens' objective perceptions of the nature of the conflict with those "informational phantoms" that are beneficial to the aggressor [11].

The priorities for the formation of an effective national security system follow from this, and above all, the formation of the worldview of Ukrainian citizens, which can be achieved only thanks to the systematic and purposeful humanitarian policy of the state and its special services. Thus, in particular, in the "National Security Strategy of Ukraine", approved by the Decree of the President of Ukraine dated May 26, 2015 No. 287/2015, it is stated that the priorities of ensuring information security are:

– ensuring the offensiveness of information security policy measures based on asymmetric actions against all forms and manifestations of information aggression;

– creation of an integrated system of information threat assessment and prompt response to them;

– countering information operations against Ukraine, manipulation of public consciousness and dissemination of distorted information, protection of national values and strengthening of the unity of Ukrainian society;

– development and implementation of a coordinated information policy of state authorities;

– identification of subjects of the Ukrainian information space created and/or used by Russia to conduct an information war against Ukraine, and making their subversive activities impossible;

– creation and development of institutions responsible for information and psychological security, taking into account the practice of NATO member states;

– improvement of professional training in the field of information security, implementation of nationwide educational programs on media culture with the involvement of civil society and business [12].

Undoubtedly, the task is arche-modern, the accents are correctly placed, the matter is to implement it in real practice. Eight years have passed since then, but the situation has not fundamentally changed. And in the "National Security Strategy of Ukraine", already approved by the Decree of the President of Ukraine No. 392 of September 14, 2020, point 20 emphasizes: "Destructive propaganda both from outside and inside Ukraine, using social contradictions, incites enmity, provokes conflicts, undermines public unity. The lack of a comprehensive information policy of the state, the weakness of the strategic communications system make it difficult to neutralize this threat." [13]. However, the practical activity of state authorities and management does not lead to a significant decrease in the level of information security of society. Waging of an information war against Ukraine by the Russian Federation showed the inefficiency and imperfection of the organizational and legal mechanism of the state security policy. Therefore, both the institutions themselves and the normative-legal mechanism for ensuring information security need reforming.

Conclusions. The conducted research gives reasons to talk about active Russian propaganda activity in the information space of Ukraine and the world. Russia's actions in relation to Ukraine have the characteristics of a "hybrid war", namely: an attempt to impose its vision on political and historical processes, establishing actual control over the Ukrainian information space, exerting influence on public consciousness by promoting pro-Russian narratives, marginalizing manifestations of Ukrainian national identity, creating networks of pro-Russian structures, parties, public associations, churches, which, through agents of influence, carry out propaganda activities on the territory of Ukraine. And as the events of 2014 and later in Ukraine showed, such organizations can potentially act as a tool to destabilize the socio-political situation within the state.

The hybrid war unleashed by the Russian Federation against Ukraine is not only a challenge to the existence of an independent Ukrainian state, the danger threatens the entire system of international and European security and leads to the destruction of the existing security architecture, discrediting its main structures such as NATO, the EU, the OSCE, the charter of the UN and the Helsinki process regarding the inviolability of borders and state sovereignty. Ukraine, as well as the entire democratic world, should respond to the enemy's aggression in a timely and adequate manner.

On the part of the state, it is necessary to constantly compare threats and dangers with the available resources for their management. A comprehensive detailing of the rights, duties, powers and responsibilities of all components of the national security management system is required. The experience of countries such as Great Britain and Germany shows that the modern "security sector" should be oriented towards meeting the challenges of future security threats instead of blindly following traditions. It should be "embedded" in a democratic society, which serves as a kind of "guarantor", i.e. ensures both internal and external information security.

References:

1. Hoffman, Frank G. (2011). Threats and Strategis Thinking. *Infinity Journal*, 4, p.17.

2. Putin's hybrid war [Electronic resource]. Access mode:http://kne/com.ua/9-glavayi-razdel/1235-gibridnaya-vojna-putina.html.

3. Magda, E. (2017). Russia's Hybrid Aggression: Lessons for Europe. Kyiv: KALAMAR, 2017, 268 p. (in Ukrainian).

4. Polevy, T.E. & Yuskiv, H.V. (2021). Russian propaganda as a tool of «hybrid aggression». Case of Belarusians. *Political life*, 3, p. 86-95 (in Ukrainian).

5. Vlasyuk, O.V. (2016). Hybrid war and its «hybrid fighters» in Ukraine: moral and political aspect Instead of conclusions / Vlasyuk O.S. National security of Ukraine: evolution of domestic policy problems: Elected Works. Kyiv: NISD, 528 p. (in Ukrainian).

6. Vlasyuk, O. (2016). Humanitarian, information and economic consequences of the war in the East of Ukraine for the European security space. Regional stability on the borders of Ukraine and the EU: modern challenges and support tools. Kyiv: NISD, p. 19-26 (in Ukrainian).

7. SACEUR: Allies must prepare for Russia hybrid war [Electronic resource]. Access mode: http // www.stripes.com/news/saceur-fllies-must-prepare-for-russia-war-1.301464.

8. Vlasyuk, O.S. (2015). Ukraine and Europe are natural allies in countering Russian informational aggression. *Ukrinform. Blogs.* July 28 [Electronic resource]. Access mode: http://blogs.ukrinform.gov.ua/blog/oleksandr-vlasyuk/ukrayina-i-yevropa-pryrodni-soyuznykyu-protydiyi-rosiyskiy-informaciyniy-agresiyi (in Ukrainian).

9. Naichuk, A.V. & Markitantov V.Yu. (2022). Key factors of the security situation in Eastern Europe and threats to the state interests of Ukraine. Political science bulletin: a collection of scientific papers. Kyiv: Vadex LLC, Issue 88, p. 175-188.

10. Horbulin, V. (2014). «Hybrid war» as a key tool of the Russian geostrategy of revenge. *Strategic Priorities,* 4 (33), p. 5-12. (in Ukrainian).

11. Batrymenko, O.V. (2022). The role of social media in the Russian-Ukrainian information war. Political science bulletin: a collection of scientific papers. Kyiv: Vadex LLC, Issue 89, p. 124-132.

12. Zakon3.rada.gov.ua/lavs/show/287/2015.

13. Https://fiu.gov.ua/pages/zakonodavstvo/392/2020/

Бібліографічний список:

1. Hoffman Frank G.Threats and Strategis Thinking. *Infinity Journal*. 2011. № 4. P.17.

2. Гибридная война Путина [Электронный ресурс]. Режим доступа: http:// kne/com.ua/9-glavayi-razdel/ 1235-gibridnaya-vojna-putina.html.

3. Магда Є. Гібридна агресія Росії: Уроки для Європи. Київ: КАЛАМАР, 2017. 268 с.

4. Польовий Т.Є., Юськів Х.В. Російська пропаганда як інструмент «гібридної агресії». Кейс білорусі. *«Політичне життя». №3, 2021. С. 86-95.*

5. Власюк О.В. Гібридна війна та її «гібридні бійці» в Україні: морально-політичний аспект. Замість висновків // Національна безпека України: еволюція проблем внутрішньої політики: Вибр. праці. Київ: НІСД, 2016. 528 с.

6. Власюк О. Гуманітарні, інформаційні та економічні наслідки війни на Сході України для європейського безпекового простору. *Регіональна стабільність на кордонах України та ЄС: сучасні виклики та інструменти забезпечення*. Київ: НІСД, 2016. С. 19-26.

7. SACEUR: Allies must prepare for Russia hybrid war [Электронный ресурс]. Режим доступа: http // www.stripes.com/news/saceur-fllies-must-prepare-for-russia-war-1.301464.

8. Власюк О.С. Україна і Європа – природні союзники у протидії російській інформаційній агресії. *Укрінформ. Блоги.* 2015. 28 липня [Електронний ресурс]. Режим доступу : http://blogs.ukrinform.gov.ua/blog/oleksandr-vlasyuk/ ukrayina-i-yevropa-pryrodni-soyuznyky-u-protydiyi-rosiyskiy-informaciyniy-agresiyi

9. Найчук А.В., Маркітантов В.Ю. Ключові фактори безпекової ситуації у Східній Європі та загрози державним інтереспм України. *Політологічний вісник: збірник наукових праць.* Київ: ТОВ «Вадекс», 2022. Вип. 88. С. 175-188.

10. Горбулін В. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Стратегічні пріоритети* . 2014. № 4 (33). С. 5-12.

11. Батрименко О.В. Роль соціальних медіа у російсько-українській інформаційній війні. *Політологічний вісник: збірник наукових праць.* Київ: ТОВ «Вадекс», 2022. Вип. 89. С. 124-132.

12. Zakon3.rada.gov.ua/lavs/show/287/2015.

13. Https://fiu.gov.ua/pages/zakonodavstvo/392/2020/

Сащук Г. М. Безпекові імперативи українського інформаційного простору в умовах гібридної війни

З'ясовано сутність «гібридної війни», як повний арсенал різних видів бойових дій (бомбування цивільної інфраструктури, тероризм, безладне, жорстоке, ніким не спровоковане насильство), так і ведення інформаційно-психологічного тиску на громадян як своєї країни так і на громадян країни-окупації із залученням державних і недержавних акторів.

Проаналізовано механізм забезпечення інформаційної безпеки України, його ефективність, як певної системи взаємопов'язаних між собою складових, від змістовного наповнення яких – від нормативно-інституційної бази наповнення – до між секторальної взаємодії суб'єктів інформаційної безпеки залежить реалізація без пекового курсу держави в інформаційній сфері.

*Продемонстровано**,** що російський підхід до інформаційної війни – це глобальна стратегія, яка включає як кібер-удари, так і інформаційні операції проти більшості демократичних акторів світу, що російські кампанії інформаційної війни продовжують дискредитацію демократичних інституцій, пропагуючи екстремізм і невдоволення, підтримуючи антидемократичних лідерів, намагаючись похитнути вплив Заходу.*

*Виявлено**,** що російські інформаційні стратегії, використовуючи широкий набір інструментів дезінформації, «фабрики тролів», тощо, спрямовані на відновлення російського домінування в пострадянській/імперській сфері впливу; зменшення впливу західних демократичних цінностей, інститутів та систем з метою створення поліцентричної моделі світу; розширення політичної, економічної та військової гегемонії Росії в усьому світі.*

Обґрунтовано, що гібридна війна, розв'язана Російською Федерацією проти України, є не лише викликом існуванню незалежної української держави, небезпека загрожує всій системі міжнародної та європейської безпеки та призводить до руйнування існуючої архітектури безпеки. , дискредитуючи такі її основні структури, як НАТО, ЄС, ОБСЄ, статут ООН і Гельсінський процес щодо непорушності кордонів і державного суверенітету.

Ключові слова: *інформаційний простір, інформаційна війна, гібридна війна, пропаганда, екстремізм, тероризм.*