DOI 10.33099/2618-1614-2024-25-2-48-57
UDC 355.4:303

M. T. Podybailo,
Candidate of Historical Sciences,
the National Defence University of Ukraine,
V. A. Fedoriienko,
Candidate of Technical Sciences,
the National University of Defence of Ukraine

Some conclusions on methods and tools of information operations: lessons of the Russian-Ukrainian war

Everyone has heard about information operations and their critical role in the structure of threats to national security does not cause objections. However, the authors in this article draw attention to the lessons and conclusions learned in the course of identifying information actions of Russians during their aggression in Ukraine. They also give examples of methods, tools and approaches used by Russians in conducting information operations at the strategic, operational and tactical levels against Ukrainian, Russian and foreign target audiences.

Key words: information operations; information and psychological impact; target audiences; methods, tools and approaches of information influence of Russia; information component of Russian aggression against Ukraine.

Introduction. If we understand that the truth needs effective tools for protection, then they must be found and implemented. A good opportunity is to take into account the current experience of using strategic lies (or as it is called – «information operations», «information wars», «measures of information and psychological impact», etc.) in the context of Russian military operation against Ukraine. If remember the basic approach that InfOps precede the use of combat units, accompany military operations and continue after the end of an active armed confrontation, a number of lessons could be made.

First of all, it should be noted that there is a certain gap in how definitions are formulated in governing documents and what is the practice of InfOps. Where are the «functional gaps» and which tools are missing or could not operate correctly. In order to demonstrate the lacks between practice and theoretical base, let's analyse some of them with brief comments starting with the most used definitions.

US Definition: «Information operations is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own» [1, p. 1–1].

Throughout the period of Ukraine's independence until the beginning the full-scale invasion in February 2022, Russia had many tools to successfully implement its informational and psychological impact on different target audiences in Ukraine. Unworried attitude and ignoring information threats as indicators of preparation for armed aggression by Russia, today is quite expensive for Ukraine and its allies.

Let's compare the different definitions of the concept of «information operations», including appropriate definitions for any specialized terminology or terms which often have varied interpretation and describe the conceptual apparatus and Russian InfOps's structure.

NATO Definition: «Information operations. A staff function to analyze, plan, assess and integrate information activities to create desired effects on the will, understanding and capability of adversaries, potential adversaries and audiences in support of mission objectives» [2, p. 14, 15].

Ukrainian Definition: «Information operation is a set of coordinated and interrelated activities for the purpose, tasks, objects, place and sometimes simultaneous and consistent measures of information influence, carried out according to a single plan and plan by the forces and means of the Armed Forces of Ukraine, involving the capabilities of the information infrastructure of the state, in cooperation with other military formations and law enforcement agencies in order to create favourable

conditions for the use of troops (forces), violation of the functioning of the enemy's information infrastructure, his decision-making processes and the management of troops (forces) while simultaneously protecting his own information space» [3, p. 13, 14].

So, in Russian documents we did not find a reference in the public domain to the concept of «Information operations» in relation to their use by the Russian army. The closest definition that characterizes the activities of the InfOps is defined as «information wars»: «Information war – a struggle between two or more states in the information space with the aim of causing damage to information systems, processes and resources, critical and other structures, undermining political, economic and social systems, massive psychological treatment of the population to destabilize society and the state, as well as to force the state to make decisions in the interests of the opposing party [4].

Research results. Describing key characteristics of Russian information warfare with verbally presented examples Riga STRATCOM COE in 2015 noted the following: escalation, dominance, speed, momentum and deception [5, p. 26].

Information and psychological impact carried out in the methods of propaganda, information and psychological operations and actions, mass gatherings (rallies, pickets), humanitarian actions, etc. The basis of the technology of information and psychological impact was misinformation, manipulation, intimidation, incitement to hatred [6, p. 159].

Information and psychological impact was carried out through different possible channels of information dissemination such as television, the Internet, broadcasting, periodicals, leaflets, rumours, etc.

The Russian authorities subordinated in their own country and created outside of it an extensive network of information resources for the exercise of information influence. And if for the member countries of NATO, as well as in Ukraine, one of the basic principles is the impossibility of conducting InfOps against their own population or partners/friends, then this principle has no limitation in Russia.

Therefore, according to the experience of the information component of Russian aggression the key conclusions regarding the generalization of these principles can be formulated as follows:

– If we identify signs of InfOps from another country, then we should consider these actions exclusively as unfriendly. And also, as preparation for other stages of the military operation for which this country is preparing.

– It is necessary to read this behaviour in such a way: this country considers us as an enemy or potential enemy and unfriendly threatening actions in the information space are, in fact, the first information stage of its military operation. Because with friends and partners the main thing in cooperation is trust. And trust is about truth.

– InfOps are not held against their own population. But the largest target audience against which Russia conducts information operations is Russia.

So, if something looks like a strategic lie, sounds like a lie, and is aggressively imposed as a systemic lie – this is called unconventional aggressive cognitive warfare with the aim of causing changes in the attitudes and actions of target audiences. If do not react to these actions in a timely manner as a threat, then it will inevitably have to repel the conventional attack.

About the effects. As in any activity, the successful results of InfOps are evaluated by the effects that have been achieved. Information effects should be measurable to provide analysis, planning, implementation and evaluation of related activities and the effects themselves [7, p. IV-9]. But not always the effects are predictable.

Russian planning and conducting InfOps is carried out on the basis of an assessment of the socio-political attitudes of the target audiences, historical memory, customs, value orientations of the population, mentality, socio-political and socio-economic situation, which is detailed in the study «Experience in the formation of a system of countering negative informational influence in the Donetsk region in the conditions of ATO / JFO» [6, p. 145–147]. The Russians made many mistakes in their calculations and became hostages of their own narrative about «one nation». They could not calculate all possible reactions of Ukrainian society. In particular, they did not foresee that the Russian-speaking population could actively support Ukraine and oppose Russian aggression.

Bottom right photo (see Fig.1) is not from Kyiv. This is March 5, 2014 in Donetsk. When the Donetsk people came out for Ukraine in Donetsk already partially occupied by Russian proxy forces. And agree, it reminds Kherson spring 2022. Although it worked too late in Donetsk, but this must be studied and taken into account. And to scale as an experience to prevent other possible situations.

The conclusion that should be drawn from this case: in 2014, both the Ukrainian authorities and NATO partner countries fell into the trap of a complex and successful Russian IPsO. Russia organized a complex of hybrid events that created the illusion of a large-scale separatist movement to the east and south of Ukraine. The media picture created by the enemy led to the adoption by the Ukrainian authorities of untimely decisions to respond to the crisis situation and counteract it.

Sociological surveys conducted in April 2014 in Mariupol, at the height of the operation «Russian Spring,» at the peak of information aggression and the actions of Russian proxy forces showed that there is a total

Figure 1. Consequences and effects of russian InfoOps in 2013–2014

difference between the situation assessment in the media and by politicians and the real mood of the population of the region. 75% of the population clearly expressed that they want to live in united sovereign Ukraine. While 20% expressed a desire to join the Donetsk region to Russia or the «Donetsk people's republic». The proportion of truly ideological supporters of separatism, and not situationally intimidated and disoriented by Russian propaganda, is much smaller, of course [6, P.150,151].

In fact, there was no any Donetsk, Lugansk, Odessa, Kherson, Mykolaiv, etc., separatisms. Only Russian hybrid aggression with a powerful information component. It is very important to name things correctly. Because if we analyse from the erroneous fact about separatism in the east and south of Ukraine, other conclusions and decisions will also be erroneous.

Analysis of Russia's actions in the context of its aggression allows us to identify the peculiarities of the applied methods and tools in the implementation of measures of informational and psychological influence on different target audiences. Russia exerts it's informational and psychological influence against its own population, against the target audiences of Ukraine and foreign countries at the strategic, operational and tactical levels.

In Russian information operations, the entire network, all actors of influence at each level are working to ensure the promotion of about ten strategic narratives against Ukraine. Thus, they create the illusion that all that information noise from the interpretation of objective events is true. Because of scale and unanimity at all levels. How does it work? According to the results of systematic monitoring of the media, social networks, collection of data on the spread of rumours in crowded places, analysis of the dynamics of sociological research, it can be summarized that Russia uses for its own purposes a group of narratives that subordinate to itself the logic of all types of communication on these topics related to Ukraine. The main techniques are strategic propaganda, lies, misinformation.

Why are there about ten topics? On the one hand, this is acceptable for assimilation by the human mind, and on the other, it is enough to create a trap: if someone doubts one of the narratives, he can get hooked by lies in one of the others. So many topics can be manipulated like a cognitive web which thrown on simultaneously at different target audiences.

10 main narratives of Russian IPsO against Ukraine:

1) «The West is using Ukraine as a testing ground in its war against Russia» («Russia is fighting NATO, not Ukraine»; «Power in Ukraine – puppets of the West»; «The West plans to divide Ukrainian territory, and Russia opposes it»; «The West wants to make Ukraine a raw material appendage», etc.);

2) «The West is already tired of Ukraine» («Negotiations to end the war»; «There will be no help»; «Internal crises begin in the West because of support for Ukraine»; «Curtailing support for refugees» etc.);

3) «Western governments simply make money on the war in Ukraine» («War is only big business»);

4) «Ukraine is the cause of world crises» («Ukrainian terrorism – «banderovtsy and nazis»; «exporting revolutions»; «migration»; «corruption»; «crime»);

5) «The Ukrainian government makes money from the war» («Total corruption», «The sale of Western aid on the black market of weapons», «Restriction of rights and freedoms under martial law», «Black transplantology», etc.);

6) «One people, one history, one faith»;

7) «Ukraine is a failed state, a project of the West as opposed to Russia» («Ukraine is not able to produce

anything on its own, everything is provided by Russia (someone else)»; «Ukraine without Russia is over»).

8) «Power in Ukraine was usurped by Nazis/fascists/neo-Nazis» («Repression of Russian speakers»; «Repression of dissidents»; «Repression of the Orthodox»; «Murder of their people»; «Biological laboratory»; «Dirty bomb»; «Eight years bombed Donbas», etc.)

9) «The Armed Forces of Ukraine are led by corrupt nationalist commanders tasked with killing as many Ukrainians as possible, after which NATO occupies Ukraine» («Cannon fodder, illegal violent mobilization»; «Problems with ammunition»; «Unprofessional air defence»; «Huge losses of personnel»; «The authorities send soldiers to their deaths to kill as many as possible»; «Demoralization of the army», etc.)

10) «Ukraine will not survive the crisis» (energy, financial, fuel, food, financial, political, mass protests, struggle for power, etc.).

Thus, every real or fictional event that is covered or commented on in public space is interpreted to serve one of these narratives. The manner of commenting is sent in the form of prepared instructions and theses to certain subjects of propaganda.

All these narratives and their subordinate topics are derived from the grand narrative: «Ukraine is a failed-state, in which, as a result of a military coup organized and paid by NATO, neo-Nazis came to power in order to separate one Russian-Ukrainian people. Russia defended its compatriots and co-religionists, who are bombed, killed, repressed by NATO through the puppet Kyiv Nazi regime because of their great language, faith and culture. That's why Russia is conducting a special military operation in Ukraine against NATO to pre-empt their plans to attack Russia first and protect its people in Ukraine».

Analysing the topics of information campaigns that Russia conducts against Ukraine, we can conclude that they are clearly classified by the goals to which they are aimed – on strategic, operational and tactical levels.

Types of channels of dissemination of negative information and psychological impact of Russia.

Until 2014, in Ukraine, the Russian had a huge network of its own legal or controlled national and local TV channels, press, websites, millions of users of controlled social networks VKontakte and Odnoklassniki, agent network at all levels of government and public life, etc.

Despite the fact that Russia's aggression against Ukraine lasted so long, the authorities only in 2017 began to introduce cautious restrictions on hostile channels for disseminating harmful information. However, these steps were partial and did not prevent enemy attacks. Radical and real counteraction started only with the beginning of a full-scale invasion in February 2022.

Of course, every time we saw these «roller coaster» of finding a balance between the observance of freedom of speech, objections from international institutions and the need to ensure national security, which restrained the authorities from decisions to impose sanctions against openly hostile channels and countering information threats. As a result, the government nevertheless came to the need to actively respond to hostile content after the start of a full-scale invasion. And today no one in the world needs to explain that this is not about restricting freedoms. But «too cautious steps» led to the loss of too much time, efforts, resources. And they cost us and our partners too much.

Conclusion: We must not forget that information operations are an integral part of a military operation. Therefore, it is necessary to react accordingly. Like an electric current. Democratic values should be with fists!

It is worth remembering that in the art of detecting and countering information attacks, approaches, channels of dissemination of malicious information, speech, etc., very often change. Therefore, the following examples are not an unambiguous instruction that should be followed unconditionally. This is only a partial generalization of experience based on the results of practical observations in the current environment.

The enemy will change the process of finding methods, channels, tools as soon as they cease to be suitable for its success. Your successful result will be luck to unravel the intentions of the enemy and destroy them. And your reward is the time you win.

The implementation of Russian InfoOps is carried out in relation to the most important strategic, operational and tactical goals, processes and actors of Ukraine. Therefore, the following examples of the implementation of real information operations (their individual elements) are in order to show their varieties relative to different targets.

Russian information campaigns, which aimed at disrupting Ukraine's achievement of strategic-level goals, concerned the military and political leadership of Ukraine – V. Zelensky, V. Zaluzhny, K. Budanov, O. Syrsky, and others. The following main cases of Russian InfoOps at this level can be distinguished: «Ukraine's membership in NATO and the EU», «nuclear threat from Ukraine», «corruption in the government», «Ukraine sells Western weapons on the black market», «grain agreement», «the West is tired. There will be no help», etc.

Case «The Ukrainian government as an object of Russian InfOps».

The President of Ukraine is a constant target of Russian information attacks. In relation to it, technologies of devaluation are used («clown,» «comedian,» «addict»). In the first weeks of the full-scale invasion of Ukraine, the Russians conducted several series of informational stuffing that Volodymyr Zelensky was frightened and fled the country. The original and easy-to-follow response

of the President of Ukraine – a photo and video message together with the main part of his team against the background of the President's office allowed to calm and inspire Ukrainian society and many people abroad (see *Fig 2*). Nevertheless, this is an important conclusion for understanding the reaction of Russian target audiences: the Russians, even after the repeated exposure of deception, did not begin to question every subsequent misinformation and strategic lies of their propagandists.

Case «Russian troops killed Ukrainian military leaders»

Another example of the strategic lies of Russian propagandists is a series of informational stuffing during a short period about the death of the higher commanders of the Ukrainian army – Generals V. Zaluzhny, O. Syrsky, K. Budanov (see *Fig. 3*).

Russian information campaigns aimed at achieving operational-level objectives relate to specific military operations (examples):

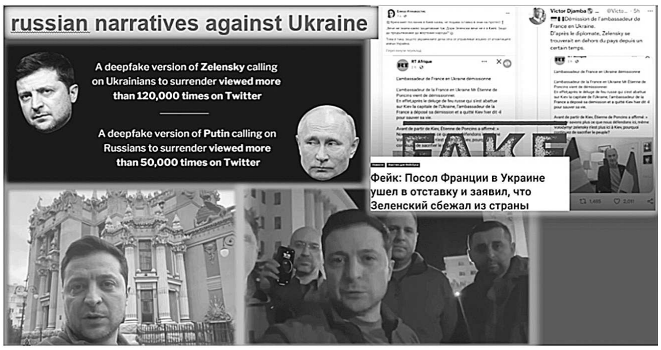

Figure 2. Russian fakes about V. Zelensky and countering them (February 2022)

Figure 3. Messages from Russian mass media and Telegram channels

– battles for Bakhmut, Soledar, etc.;

– destroyed the dam of Kakhovka water reservoir, the sinking of the cruiser «Moscow», etc.

This is a classic accompaniment of specific operational actions, which is well known from operational art. Its task is to demoralize, mislead, impose certain decisions on the enemy side during a military operation.

Cases of Russians informational and psychological influence on local target audiences: SMS mailing, leaflets, content in local chats and groups in social networks, at meetings with calls for certain actions, misinformation about situations and conditions on local issues that are critical for the community and person life, calls for illegal actions in order to produce tension, hatred, aggression, fear, etc.

The best sign of skill, as it seems, is the ability of a specialist to identify the intentions of the enemy in a timely manner and at the tactical level. The following are some relevant examples of cases, methods and tools that Russia uses in the implementation of information effects on the tactical level. Therefore, we will dwell in more detail on examples of the tactical level of implementation of information measures, techniques, tools of Russians.

Mass SMS mailing. This is one of the most frequent ways that the enemy uses to penetrate information to our target audiences.

Most often they are aimed at the military and the population of the front-line territories. Arrays of anonymous messages through Internet gateways are sent to all numbers which have been identified in a certain territory. Their goal is not only to exert psychological pressure, but also to induce certain actions. In the photo (see *Fig. 4*) – one of the examples this newsletter, which the Russians massively distributed in the area of Mariupol and Berdyansk on May 21, 2018.

Conclusions. It is very important for specialists working with the assessment of enemy information actions to understand the steady state of the local information environment (the concept of norm). After

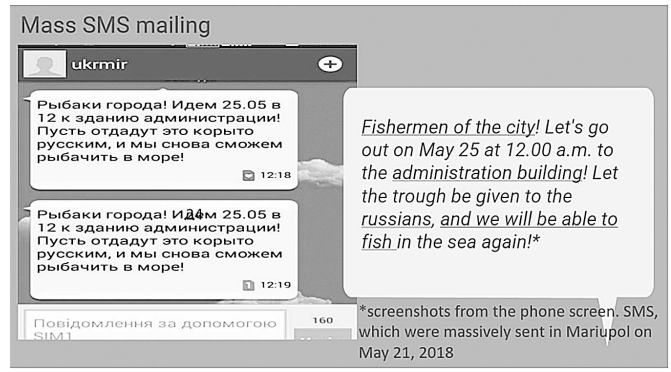

Figure 4. Mass sending of messages to detected phone numbers

analysing this specific example, signs of active actions of the enemy were identified, which, together with the subsequent data collected, made it possible to make timely decisions on countermeasures.

This particular message attracted attention due to the presence of «signs of alien» (interference in the local information space by third parties who do not sufficiently understand the local specifics, with the aim of manipulating the target audience). In particular, the fact that the goal of the «alien» was to destabilize the socio-political situation was evidenced by a number of well-known local facts. Namely, the local residents would not be able to understand which «administration» it was necessary to gather for the protests, because in Mariupol there were four district, city (which did not work since the Russian proxy forces burned it back in 2014) administrations, as well as the administrations of factories and the Mariupol port. And the alleged attempt to gather people in the city centre near the city council building was also not «read» by the residents, as they usually called in short this administration building the «city executive committee» [gorispolkom].

Another marker that pointed to the work of non-locals was the choice of the target audience without understanding the real circumstances of their lives. After all, the ship «Nord» stolen by the Russians in Crimea, which was arrested by the Ukrainian coast guard, was in the port of Berdyansk. And the local fishermen had no idea about him. And that is why they definitely could not reflect on this call for protests against the Ukrainian government.

That is, despite the density of distribution (significant resources were involved), the text messages contained a number of signs indicating intentions to destabilize the situation, and the information obtained, as a result of the analysed signal from these messages, about the Russians conducting exercises in their waters of the Sea of Azov, finally confirmed the information stage of the Russians' military operation.

But at the same time, the enemy's specialists made one of the typical mistakes – they acted in a formulaic way, but without understanding the specifics of the territory and toponymy. Thus, the understanding of the stable state of the local information environment in combination with the obvious own network of chats and groups of the local population, focused on the detection of strange information signs, as well as work in the format of a situation centre with other services and structures, made it possible to effectively identify the beginning of aggressive actions of the enemy at an early stage.

Leaflets. The technology of informing using leaflets is well known and does not require description. In the context of our tasks, an example with leaflets is given in view of the technology of their distribution (see *Fig. 5*).

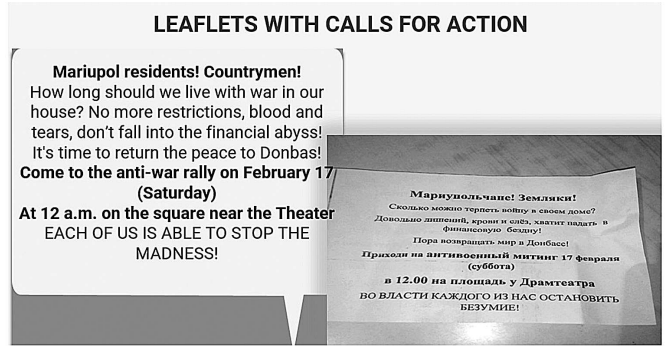

Figure 5. Leaflets that were distributed in Mariupol in public places and in entrances of houses in February 2018

Young people who read the ads in a local group on the social network are involved in their distribution. They contacted the customer remotely. And they took up this work simply because «they did not see anything anti-Ukrainian in this task». They were given written simple and clear instructions: print the sent text on a regular printer, distribute it in certain places, send a photo report to the customer. According to the results – to receive payment on a bank card.

One of the important conclusions: do not expect that ordinary people are able to recognize threats. Especially if they want to make money. Most people expect simple answers to complex questions. They do not see hostile manipulation. Therefore, they are ready to «stand for all good against all bad». Or as they say: «Only there was no war!» Not realizing that they themselves are becoming an instrument of this war.

Local Social Media Groups.

Another example of mass influence on the consciousness and activity of people is local closed groups. You have to make an effort to get there. Because moderators follow who they add.

That is why communication should be established with a pool of volunteers who should know that they must join these groups and should report when they start talking about something threatening. Therefore, you need to give the basics of media literacy. Because the enemy in his manipulations often disguises harmful content (see *Fig. 6*).

What are the local groups? Parent groups in schools and kindergartens, corporate groups, neighbours' chats, etc. That is, where people are connected by narrow, but critical interests for themselves. Therefore, when even a rather strange message appears, it will be read here and there is a possibility that it will cause confidence.

So, it's very important to build a system in which such threatening information will get to you as soon as possible. To be able to unravel the plans of the enemy!

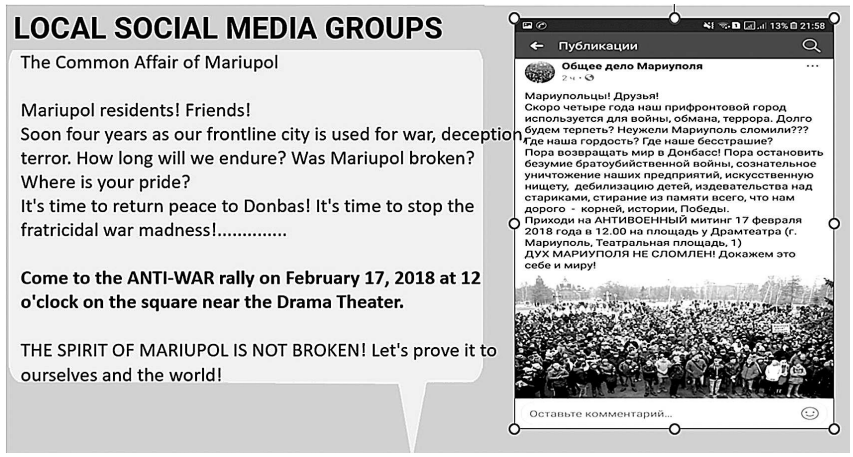

Figure 6. Messages in the network of inspired local groups in messengers

Bot Farms.

Old familiar bot farms. Everyone knows how they work. But the key word – they still work! And yes, they can do harm if not counteracted (see *Fig. 7*). One of the most effective ways to counteract is to identify and highlight information about bot accounts in the comments, instruct people not to react to them, not to enter into a discussion. And, of course, fix networks to try to block them.

Process of History Simulation.

This is a very effective tool. If the society has lacunae of historical memory or identity problems that are not filled with the family upbringing, education, memory policy, there are no responsible community leaders and there are many other circumstances that complicate the situation, then the enemy will certainly take advantage of this condition deprived of immunity!

Figure 7. Bot farms mechanically generate threatening content, which is often detectable

It turns out that people who do not have their own clear beliefs are very easy to integrate into another reality. To another «truth». The one who communicates is easily disorienting. Especially when the situation is stressful and incomprehensible for them. Because under stress, people need explanations. Especially if this state of stress is created for them. And we have seen many such artificially created situations before and during the war. But in recent years, we have seen progress. If we form the information stability of society by means of strategic communications, consistently and openly implement the policy of memory, then people are much less susceptible to such hostile influence. False history is a tool of Russian InfOps. For their own and foreign audiences, Russia widely implements these basic narratives depriving Ukraine and Ukrainians of historical subjectivity. Everyone remembers Putin's historical passages that «Ukraine never existed» [8]. Nonsense, which can be perceived only by those who do not know the history of our people at all, or just inclined to think so, contrary to reality.

And from this it is worth drawing another conclusion from this case: Ukraine is also to blame for such a situation. After all, for many years Russians, the world, and even Ukrainians have heard only this Russian propaganda. Ukraine did not sufficiently fill the information vacuum about its own picture of the world.

Important conclusion! Russia always works where there is an information vacuum!

You can see in the photo of 2005 the beginning of Russian aggression (*Fig. 8*). A few marginal alcoholics with pro-Russian sentiments. They were invisible and not understandable to the local population. Nobody knew about them. They had no support. During the period from 2005 to 2014, several inconspicuous actions were held. But this and several similar photos were used to scale

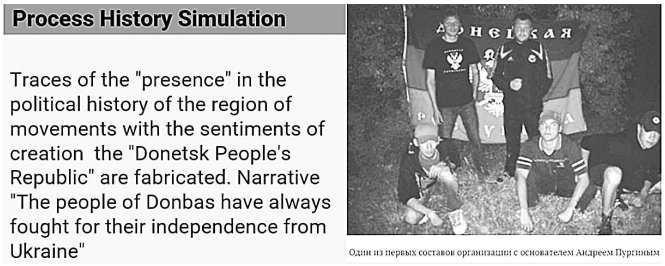

Figure 8. 2005. Extremist organization «Donetsk People's Republic» in full force

their tasks by Russia as evidence: «The people of Donbass have always fought for independence from Ukraine. Or for the «idea of one people».

Crucified boy in Slovyansk.

And another example of a tool that is very often used by Russians in the spread of information and psychological impact. Everyone knows him as «The story of the crucified boy in Slavyansk». The effect was incredible (see *Fig. 9*).

Russia, actively using the trust factor of a significant population part to the TV, widely applies video content of various types. Scaling the effect of the effect is due to the technology of repeating «especially important news», intimidation through emotional methods of forcing in propaganda «educational» programs such as «Top Secret,» talk shows such as «60 Minutes with Olga Skabeeva,» etc., which use many manipulative methods of influence and persuasion. However, in recent years there has been a significant shift not only in Ukraine but also in European countries. And now they pay great attention to checking information and identifying fakes and to media literacy.

Now this story has become a meme. But in 2014, many people believed that this was true. This technique is still widely used by Russia. The more ridiculous the lie, the easier it is to believe the masses. The technology actively continues to work. On other topics. And if Ukrainian society is vaccinated against it, then the target audiences of such «series» are now often – foreign communities and always – Russians. Everything happens according to the scheme: «resonance in the news release – discussion on talk-show – detailing in the «educational» programs with elements of mystification (conspiracy theory)».

Figure 9. Still shot from a Russian propaganda interview about the «crucified boy in Sloviansk»

Some new techniques and tools of Russian InfOps. Russia is constantly updating its methods and tools of influence on the consciousness of different audiences. And most importantly, this will continue all the time!

We will find ways to counter some threats, and they will look for others. Therefore, the ideal system of countering information threats, with a properly built system of information stability, should be implemented at the tactical level. It is there that they must be detected and neutralized. The initiative at the strategic and operational level should be on our side. Again, under the conditions of an effectively implemented system of information stability.

Here are some relatively new techniques that Russia has begun to use, given its resistance to traditional channels and instruments for spreading its threatening influence.

Recently, we regularly began to meet ambiguous and incomprehensible materials that are distributed with reference to quite authoritative publications.

It is clear that if the blog of an independent media person is posted on the website of a respected publication, then the easiest way is to miss the mention that this is a private opinion, but you just need to indicate the name of this respected media. Given that due to the large number of sources of information, the peculiarity of today's time is the reluctance of people to turn to the original source, most consumers of content will remember that a certain authoritative publication commented on certain events so odiously and unusually. Our behaviour, under the influence of changes in emotions (surprise, doubt, fear, etc.), will also change.

Recently, The Guardian published information (see *Fig. 10*) about how an employee of Radio New Zealand edited materials from the BBC and Reuters, adding pro-Kremlin content to them (see *Fig. 8*). An investigation is underway [9].

In particular, the Revolution of Dignity in the materials is called a «coup» and a «civil war». In some places, whole paragraphs have been added that justify Russian aggression against Ukraine and argue that the attack was a response to the «threat to Russia and the oppression of the Russian-speaking minority».

Often there are consonant and similar in design English-language publications. Like, for example, FoxNewsRussia. Increasingly, Russians are using fringe foreigners to relay their own narratives and criticize Western support for Ukraine to show that not everyone in the West unequivocally approves of Western support for Ukraine. Sowing doubt is the first step: break alliances and provoke destabilization. We remember that

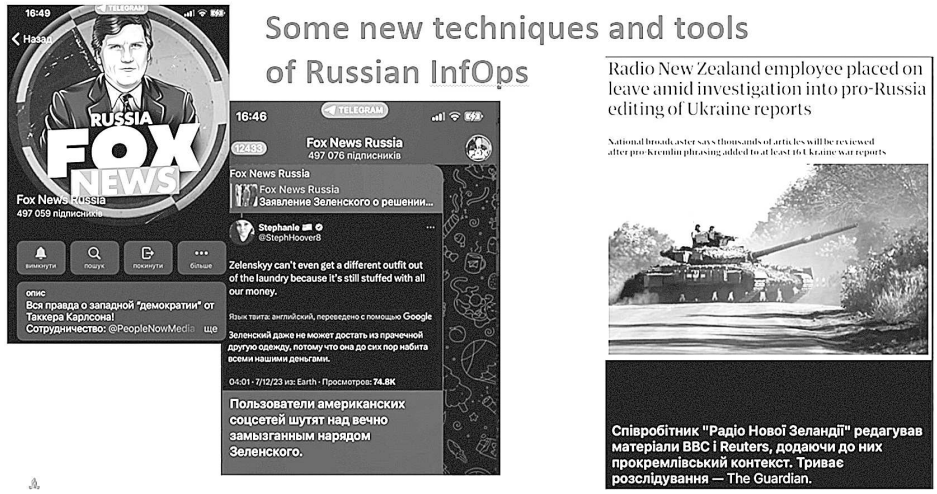

Figure 10. Using well-known media to inspire fake content

the emotion of doubt became revolutionary when the dominant dogmatization of scholasticism in the Middle Ages was replaced by the ideas of the Enlightenment and humanism. That is, it can be summarized that these techniques of «sowing unrest and heresy» can successfully work in the direction of the target audiences of the enemy. The main thing in this matter is proactive, not just reactive actions.

Another new tool that is increasingly used by Russians is the use of artificial intelligence for content production. So many viral videos featuring disinformation about the military have surfaced online. Especially effective for the enemy is the production of video sequences and dubbing products of an allegedly demonstrative nature about the military and politicians. One of the most common technologies is deep fake.

At the same time, AI has formalized approaches to the selection of information and, often, does not compare or verify facts. It generates content on formal grounds. In war conditions, there are a number of factors that allow you to bypass or complicate the quality of AI and simplify the detection of information threats. This is due to the limitation in public space of many peacetime data usual.

However, AI learns quickly. Therefore, it is worth developing a mirror approach in this activity, and looking for ways to manoeuvre.

Therefore, in the work on identifying information threats, it is worth being mobile and attentive to details.

Often in the work of monitoring services there is a practice when scientists monitor the static list for a long time, do not change the protocols. Often without taking into account the fact that the channel has already lost its relevance and new channels for disseminating information have appeared and new keywords or new topics for search have appeared. In this regard, *we are convinced* that the role of experts who regularly monitor the information space will be preserved even with sufficiently advanced and convenient automated monitoring services. The expert with his own experience and systematic monitoring of the information environment is able to notice new trends, technologies, phenomena and channels of dissemination of threatening information. Do not rely only on software products!?

Summing up. Key principle worth remembering: global information resilience consists of the sum of local/personal resiliences. Therefore, if we work with threats from issues in national or international media, we missed these threats. Missed a punch. At the tactical level. Where it is easier to manage crisis situations.

The enemy will always look for our information gaps and weaknesses to carry out/try to carry out information and psychological impact on target audiences as a stage/part of its military operation. Therefore, it is necessary to constantly study the characteristics of all target audiences, identify and develop those that may become vulnerable to enemy influence. And also carry out systematic and adequate monitoring of the information space state, analyse and assess the level of information threats!

Thanks to systematic and comprehensive monitoring, understanding of the structure of the information environment and the characteristics of target audiences, information threats should be identified as early as possible! And the answer to them is timely, and better – preventive. This is possible with high motivation, staff training, a reasonable approach to building systematic work and a responsible attitude to the performance of their duties.

One of the biggest mistakes was to ignore a key part of statement that InfOps is an integrated component

of military operations. Therefore, at the moment of revealing signs of such operations by Russia against Ukraine (and other countries too), it should have been considered as the beginning of military aggression, and not just as «certain unfriendly competitive actions».

Remember that information operations continue until the beginning of the armed confrontation, accompany them and continue after their completion. They continue all the time. Therefore, they need our constant attention.

References

1. The Conduct of Information Operations [Електронний ресурс] : ATP 3-13.1 : October 2018 / Headquarters, Department of the Army // Army Publishing Directorate. – Режим доступу : https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN13138_ATP 3-13x1 FINAL Web 1.pdf.

2. Allied Joint Doctrine for Information Operations : AJP-10.1 / NATO Standardization Office. – Edition A, Version 1. – [Brussels] : [NSO], 2023. – 110 p.

3. Словник військових термінів та скорочень (абревіатур) : ВКП 1-00(01).01 / Воєнно-наукове управління ГШ ЗС України. – [К.] : [ГШ ЗСУ], 2020. – 52 с.

4. Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве [Електронний ресурс] / Министерство обороны Российской Федерации. – Режим доступу : https://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle#1.

5. Analysis of Russia's Information Campaign against Ukraine. Examining non-military aspects of the crisis in Ukraine from a strategic communications perspectives [Електронний ресурс] / NATO StratCom Centre of Excellence. – Riga : [NATO StratCom Centre of Excellence], 2015. – 40 p. – Режим доступу : https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf.

6. Подибайло М. Досвід формування системи протидії негативному інформаційному впливу у Донецькій області в умовах АТО/ООС / М. Подибайло, О. Українцев // Стратегічні комунікації в умовах гібридної війни: погляд від волонтера до науковця : монографія / [за ред. Л. Компанцевої] ; Національна академія Служби безпеки України. – К. : НА СБУ, 2021. – 499 с.

7. Information Operations [Електронний ресурс] : Joint Publication 3–13 : 27 November 2012 / Joint Chiefs of Staff. – Incorporating Change 1, 20 November 2014 // Federation of American Scientists. Intelligence Resource Program. – Режим доступу : https://irp.fas.org/doddir/dod/jp3_13.pdf.

8. Путин – детям: Украины не существовало [Електронний ресурс] // Корреспондент.net. – Режим доступу : https://korrespondent.net/world/russia/4511874-putyn-detiam-ukrayny-ne-suschestvovalo.

9. McClure T. Radio New Zealand investigates Russia-friendly editing of Ukraine articles [Електронний ресурс] / T. McClure // The Guardian. – Режим доступу : https://www.theguardian.com/world/2023/jun/09/new-zealand-outlet-investigates-russia-friendly-editing-of-ukraine-articles.