INFORMATION WARFARE AS AN INTRODUCTION TO RUSSIA-UKRAINE ARMED CONFLICT

Dejan Vuletić[1]
Miloš R. Milenković[2]

DOI: https://doi.org/10.18485/isimod_strint.2023.ch11

Keywords:
Russia,
Ukraine,
armed conflict,
hybrid warfare,
information warfare

Abstract: *After the collapse of the USSR, Ukraine was the area where and around which the interests of Russia and Western powers, primarily the US and NATO, clashed. Two "colour revolutions" in the 21st century best illustrate the dynamics of political balance changes and the influence of external factors in this European state. The conflict between Russia and Ukraine, particularly after the Russian annexation of Crimea, is viewed as a "hybrid warfare", whose significant component is, among others, "information warfare". This paper considers the characteristics of the information warfare that preceded the Russian armed aggression against Ukraine. Russia has been preparing for a long time and has shown great efficiency in information warfare in the period until the beginning of the current armed conflict. The Russian sphere of influence was global. Various forms of information warfare (cyber, psychological propaganda, electronic, intelligence, etc.) have been combined. The action in information space was characterized by the integration of various resources, dynamism and flexibility of their use. The Russian information operations in Ukraine can be characterized by a high level of sophistication and their complex character. In the confrontation with Ukraine, Russia had numerous advantages from the aspect of controlling information space: technical tools, vast experience, as well as long-term practice in conducting information operations. The lessons*

[1] Dejan Vuletić, PhD, research associate, Strategic Research Institute, University of Defense in Belgrade, Veljka Lukića Kurjaka 1 St, 11000 Belgrade, +38111/3603-480, dejan.vuletic@mod.gov.rs
[2] Miloš R. Milenković, PhD, research associate, Strategic Research Institute, University of Defense in Belgrade, Veljka Lukića Kurjaka 1 St, 11000 Belgrade, +38111/3603-470, milos.milenkovic@mod.gov.rs

learned in the conflict with Georgia in 2008 were particularly useful. On the other hand, Ukraine proved to be unprepared for information warfare and the undertaken measures were, for the most part, reactive. The impact of social networks, various mechanisms for compromising information infrastructure, as well as unmanned platforms, were very significant.

From ”the colour revolutions” to an armed conflict

The relationship between two close East Slavic nations, Russians and Ukrainians, who shared the common past and lived in the common state for centuries, once in Imperial Russia and later within the Soviet Union, is quite complex, and it has reached one of the lowest points in history with the current armed conflict. The dissolution of the Soviet Union in 1991 into fifteen states, which were autonomous republics until then, marked the end of the Cold War at the same time. This led to the fact that about 22 million Russians found themselves out of the territory of the Russian Federation, most of them in Ukraine. The term ”Russian” could also refer to someone ”who only speaks Russian, and is not of Russian origin, or identifies themselves with the Russian state or culture” (Samardžić, 2021: 159). After the separation, Ukraine and Russia have continued to function as independent states; they had intensive cultural, economic, political and military cooperation. However, in recent history, the overall relations between Russia and Ukraine, especially at political and security level, have been oscillating, and after Euromaidan in 2014, these relations have taken on an extremely negative character and a trend that culminated in the Russian aggression against neighbouring Ukraine.

What cannot be denied is that since the collapse of the Soviet Union, Ukraine has been at a kind of political crossroads between pro-European and pro-Russian politics. This dilemma of the state strategic foreign policy orientation has deeply divided Ukrainian society in which, according to the 2001 census, about 17% of the population declared themselves ethnic Russians (the greatest in Crimea), about 30% spoke Russian, and a large number belonged to the Orthodox Church under the jurisdiction of the Moscow Patriarchate (Constantin, 2022). More serious signs of political instability in the context of this division are the elections between two presidential candidates of different political views; one oriented towards the East and Russia, and the other towards the West and the US. A series of protests and political events from the end of 2004 and the beginning of 2005, which were related to the election process, is known as the Orange Revolution. Namely, the results after the second round of the presidential elections, in which Prime Minister Viktor Yanukovych, who was otherwise pro-Russian, officially won, were disputed by his opponent Viktor Yushchenko and the pro-Western opposition, claiming that such a result was the consequence of the election fraud. This

sparked off massive street demonstrations, after which the Supreme Court of Ukraine ordered a repeat of the elections and Yushchenko won. These elections were important, not so much because of the democratization of Ukrainian society, but because of the question of which party will exercise influence in this European state, Russia or the US, together with the European administration in Brussels.

Immediately after the Orange Revolution, Ukrainian official foreign policy priorities included joining NATO. Due to the opposition of Russia, which considered it a threat to its security, and also due to the obligations arising from the Friendship Treaty with Russia, Ukraine has postponed this decision. Due to the fact that in Ukraine itself there has always been a deep division over its membership in NATO, which has greatly destabilized its political scene, it saw a way out in the policy of balancing between the US and the EU on the one hand and Russia on the other (Jović-Lazić, 2015). The political turmoil has soon spilled over into the field of economics, that is, energy industry. It is well-known that Russia is very rich in energy resources and that, in addition to economic benefits, it often uses them for political purposes, as well. Despite the political upheaval, gas has continued to be the main means of the Russian influence in Ukraine. Thus, on two occasions, in 2006 and 2009, the gas supply from Russia via Ukraine was interrupted, jeopardizing not only Ukrainian, but also European market. Despite the official explanation that the problem arose due to a disagreement over the gas price, many saw it as the Russian pressure on Ukraine due to its pro-Western course (Jović-Lazić and Lađevac, 2018). The increased tensions between the two neighbours in those years were also caused by the issue of Crimea, i.e. the use of ports for the Russian Black Sea Fleet. In the period from 2007 to 2011, Ukraine conducted intensive negotiations with the European Union on the Association Agreement, which was already agreed upon the following year. However, the Government of Ukraine made a decision to suspend preparations for the signing of the Association Agreement, which was supposed to be signed at the Eastern Partnership Summit in Vilnius at the end of 2013.

Such a decision was the reason for new mass demonstrations from the end of November 2013 to February 2014 and an introduction into a new political upheaval known as Euromaidan. Due to the political crisis caused by mass demonstrations and the violent takeover of local governments across Ukraine, Prime Minister Mykola Azarov resigned. In an attempt to calm the situation, pro-Russian President Yanukovych offered the position of Prime Minister to the opposition, but his proposal was rejected and his resignation was demanded. In fear of his safety, Yanukovych left Kiev, and on the following day, February 22, 2014, the Parliament of Ukraine, contrary to the Constitution, dismissed him from the presidential function, which officially ended Euromaidan. Three months later, pro-Western candidate Petro Poroshenko was elected president. Ukraine signed the agreement with the EU on June 27, 2014, and on June 12, 2020, NATO granted Ukraine the status of the Enhanced Opportunities Partner.[3]

[3] "The North Atlantic Council recognised Ukraine as an Enhanced Opportunities Partner. This status is part of NATO's Partnership Interoperability Initiative, which aims to maintain and deepen cooperation between Allies and partners that have made significant contributions to NATO-led operations and missions" (NATO recognises Ukraine as Enhanced Opportunities Partner, 2020).

Having in mind the actors, technique and the method of execution, it can be said that the Orange Revolution and Euromaidan are actually ”the colour revolutions”, which have resulted in an unequivocal political turn of Ukraine towards NATO and the EU. ”The colour revolutions” are never just spontaneous gatherings of citizens, but well-planned campaigns with clear and highly focused messages and goals, and as a rule, they are externally supported (Milenković and Mitrović, 2019). In the geopolitical sense, both of these ”colour revolutions” represent the victory of the US over Russia, which was very frustrating for the Russian political leadership. The Russian reaction to this kind of political change at the beginning of 2014 was the annexation of Crimea after the referendum held on March 16, 2014, which the Ukrainian authorities did not recognize. Already next month, there was an armed rebellion in the eastern parts of the state made up of the majority Russian population, which does not want to accept the new government in Kiev. Countering this, central Kiev authorities undertook the military action in order to quell the rebellion in the Donbass and re-establish full control over the eastern regions, leading to a more massive internal armed conflict. The establishment of the self-proclaimed states of the Donetsk and Luhansk People’s Republic, which had the Russian support at the time, further deepened Ukrainian-Russian enmity (Walker, 2023).

In attempts to solve the security crisis in the state, the newly elected Ukrainian President Petro Poroshenko, as well as his successor Volodymyr Zelenskyy, are trying to gain the support of leading Western countries. The new National Security Strategy of Ukraine, which was signed by current President Zelenskyy on September 14, 2020, has foreseen, inter alia, more intensive cooperation with Western partners and ”the development of a special partnership with the North Atlantic Treaty Organization in order to obtain Ukrainian full membership in NATO” (Стратегія національної безпеки України, 2020). This was just another confirmation of the justification of the Russian fear of NATO expanding to the East and approaching its borders, which is why Russia has undertaken more serious actions in order to improve its security, protect its external borders and preserve its sphere of influence in the post-Soviet territory. This time the answer was the Russian aggression against Ukraine in the morning hours of February 24, 2022, or, as Putin euphemistically called it in his address, ”a special military operation” with the aim of ”the demilitarization and Denazification” of Ukraine (Putin’s address, 2022).

Information warfare as the content of ”hybrid warfare”

According to some theories, activities that lead to the state destabilization, or to the overthrow of the government in it, with the aim of establishing a new, changed state that disrupts the established balance of power in international relations in order to achieve one’s own interests, and which are carried out mainly by non-combat means, can be called hybrid (Kofman and Rojansky, 2015). Hybrid security threats are actually all phenomena that involve the synergistic use of conventional weapons, unconventional and irregular tactics, terrorist acts and criminal activities,

simultaneously acting on a battlefield, with the aim of achieving political goals (Hofman, 2007). As the content of hybrid warfare, numerous activities that affect different spheres of social actions are recognized, including information warfare and the already mentioned ”colour revolutions” (Mitrović and Nikolić, 2022).

One of the characteristics of hybrid warfare is that in addition to state and its authorities, (violent) non-state actors also appear as conflict actors. Violent non-state actors can be used as intermediaries in pursuit of the interests of a state that sponsors them. ”By acting via intermediaries, governments get the opportunity to achieve their goals, both within the borders of their state and abroad, violating their laws, international norms and signed contracts” (Milenković and Subotić, 2017: 60). In such a way, before the beginning of the direct conflict between the regular Armed Forces of Russia and Ukraine, the fighters of the so-called Donetsk and Luhansk People’s Republic, which have had the support of Russia since the first days of their actions, have been perceived.

Although the term ”hybrid warfare” has been known to the scientific and professional public for a long time, it became particularly frequent after the Russian annexation of Crimea, in order to describe the conflict between Russia and Ukraine. Analysing the events from 2014 onwards, one can often hear the view that Russia waged a ”hybrid warfare” in Ukraine that combines ”cyberwarfare, a strong disinformation campaign and the use of highly trained special forces and local rebels” (Samardžić, 2021: 190). In addition to Ukraine, the European Union was also targeted by the Russian ”hybrid warfare”. ”Russia has become increasingly aggressive in cyberspace, where it has exploited dissatisfaction with economics, politics or social status by spreading deception and fake news, primarily to create confusion and inflame fears in the EU” (Samardžić, 2021: 196). It is estimated that this action of Russia and a kind of indecision in the field of the EU foreign and security policy has led to the strengthening of populists in the Union itself, even in its immediate periphery.

The expansion of information warfare began in the 20th century with the development of information and communication technology. ”Information society is characterized by a high level and speed of transmission, reception and exchange of digital data and information” (Vuletić and Đorđević, 2022). ”Information and communication technology affects every aspect of the lives of individuals and communities, relations between states and their security” (Vuletić and Đorđević, 2021). The development of information and communication technology has enabled achievements in weapons and related equipment that has influenced the change in the manner of warfare.[4] The history of conflicts testifies to many examples that indicate the importance of information and achieving informational superiority over the opponent (FM 3-0, 2017). In information warfare, information is used as a weapon to influence the perception of the opponent, to subdue their will to fight instead of physical force. ”Information enables the optimal functioning of the decision-making process of military

[4] The term ”war” represents a state of armed conflict between different countries or groups within a particular country, while ”warfare” implies engagement or activity related to conflict.

commanders" (Vuletić and Stanojević, 2022). Information action affects the will, morale and perception of the opponent's decision-makers and other participants in operations, information flows that serve as support in the decision-making process, which directly affects the adversary's combat capabilities.

The activities in the information space between Russia and Ukraine

The experience that Russia gained from the conflict with Georgia in 2008 spoke about the importance of the internet, social networks, blogs and similar platforms, as well as the issue of the time of initiation of informational action (attack). During the short conflict between Russia and Georgia, attacks on information infrastructure were launched simultaneously with military operations on the ground. Georgia effectively opposed Russia in information space, which has undoubtedly influenced the change in the conduct of subsequent operations. Russia adapted its informational confrontation strategy six years later against Ukraine, seizing Crimea quickly and without much resistance and keeping potentially intervening countries at bay. It is clear that Russia has dominated information space, which has been used to strengthen its propaganda, messaging and disinformation capabilities in support of geopolitical goals. Unlike the simultaneous digital and armed attacks in Georgia, cyber attacks on Crimea degraded telecommunications infrastructure, disabled *web*sites of many institutions and jammed the mobile phones of key Ukrainian officials before Russian forces entered the peninsula on March 2, 2014 (Unwala and Ghori, 2015; Iasiello, 2017).

Russia has been preparing for a possible armed conflict with Ukraine for years. Ukrainian media experts Vitaliy Moroz and Tatiana Lebedeva believe that it started developing the idea of dividing Ukraine into two or three parts about twenty years ago. In addition to an extensive information campaign at all levels (e.g. on television, social networks, in newspaper articles), the gas disputes emerged as a part of intensified information warfare against Ukraine (Holger and Sazonov, 2018). The goal of Russian information warfare was to undermine Ukrainian society internally by discrediting leading political figures, diverting Ukraine from the course of European and Euro-Atlantic integration, encouraging social discontent and separatist feelings and justifying the protection of compatriots in Ukrainian territory. The primary goal was the destruction of Ukrainian statehood, the denial of Ukrainian identity, language and culture (Pashkov, 2016).

Until 2013, Russian information campaign against Ukraine was in the preparatory phase, which included an informational study of the situation. A much more aggressive phase followed, in the autumn of 2013, on the eve of the EU summit in Vilnius, where the Agreement on Ukraine's accession to the European Union was to be signed. The main difference in terms of information war before the seizure of Crimea and after it is reflected in the fact that Russia took the position of Eastern

Ukrainians in the period after 2014 (Pashkov, 2016; Muradov, 2020). Russian information war against Ukraine was aimed at the pro-Russian population of the industrial regions of Ukraine, primarily civil servants, intellectual elite and the elderly population. Moreover, it was heavily involved in social networks, where pro-Russian messages were distributed. The Russian Federation continued to conduct special information operations throughout Ukraine, using a wide variety of channels, including media resources and social networks.

In the confrontation with Ukraine, Russia had numerous advantages in terms of controlling information space: technical tools, vast experience, as well as long-term practice in conducting information operations (Pierzchała, 2019). It has made a great effort to increase its media presence in Russian-speaking areas along its borders. Moreover, in both Crimea and Eastern Ukraine, it decided to take over the media companies so that it could control the content that was broadcast. The Russian government's sphere of influence was global. Many propaganda campaigns were carried out in Russian, English, Arabic, French, Czech, Georgian and other languages (Angevine et al., 2019; Helmus et al., 2018).

Russia was also engaged in a very intensive campaign aimed at several different regions, including its neighbours. Social media was by no means the only platform for this campaign. It synchronized actions on social media with actions via TV stations, portals, civil society organizations (Helmus et al., 2018). Many Western scholars have labelled Russian tactics in Ukraine as hybrid warfare, the use of hard and soft techniques that rely on proxies and surrogates to prevent attribution of certain activity to the Russian party, conceal intent and maximize confusion and uncertainty (Iasiello, 2017). The Russian informational campaign in Ukraine in 2014 was a massive, multifaceted, responsible and coherent operation. The military activities were supported by an active media campaign that undermined the Ukrainian authorities and their political goals to reunify the state. The Russian information activities skillfully targeted a wide range of population that had different beliefs and convictions. In addition to the content of messages, Russia controlled the availability of information (i.e. by controlling TV and radio towers, mobile phone operators, etc.) (NATO Strategic Communications Centre of Excellence, 2016). The Russian leadership has long understood that it is impossible to achieve the desired effects simply by setting up certain *web*sites or displaying the comments of trolls. The reported news was prepared much earlier. The promotion of content was facilitated due to many similarities between the populations of both states (Muradov, 2020). The Russian informational tools for persuading the public were diverse and included historical myths, narratives and symbols. One of the most effective and frequently promoted narratives was the Soviet victory in World War II (Holger and Sazonov, 2018).

Before, during and after the annexation of Crimea, cyber espionage provided important information that enabled the achievement of objectives (Iasiello, 2017). Cyber espionage operations represented a significant segment of information collection and influenced subsequent events. Unlike the espionage in Georgia, cyber espionage was aimed at computer systems and accounts of journalists in Ukraine, Ukrainian information infrastructure, resources and accounts of officials of the North

Atlantic Organization and the European Union. By achieving such goals, Russia had insight into opposing journalistic narratives, as well as inclusive diplomatic initiatives. Many examples emphasize Russian intensive activities in information space. Operation Armageddon, in mid-2013, for example, aimed to discredit and compromise the Ukrainian government, military and police officials. As in Georgia, some groups, such as *CyberBerkut*, have also participated in various cyber attacks on Ukraine. This group carried out distributed denial-of-service attacks and compromised *web*sites of various Ukrainian and NATO institutions, intercepted documents on the US-Ukrainian military cooperation and attempted to influence the Ukrainian parliamentary elections by disrupting the information systems of the Ukrainian Central Election Commission. The attacks contributed to a general confusion in Ukraine. Stolen information ”leaked” to the public, such as a telephone conversation between the US Assistant Secretary of State Victoria J. Nuland and the US Ambassador to Ukraine Geoffrey R. Pyatt, which, in a way, negatively affected the US rating in the world (Iasiello, 2017).

Furthermore, Russian great activity was carried out on social networks (first of all, the most popular in the post-Soviet space Odnoklassniki and Vkontakte), where pro-Russian messages were distributed. The Russian Federation continued to conduct special information operations throughout Ukraine, using a wide variety of channels, including media resources and social networks. Russia has used social media as an effective tool to manage public perception (Szwed, 2016; Muradov, 2020). In addition to the above-mentioned, most commonly used social networks in the post-Soviet space, important activities also took place on other, global social networks such as *Twitter*. A record of 900,000 tweets in the second quarter of 2014 coincided with the escalation of the conflict in Eastern Ukraine. The Russian trolls were particularly active after the crash of *Malaysia Airlines Boeing-777*, which took flight MH17 from Amsterdam to Kuala Lumpur. The plane was brought down on July 17, 2014 in Donbass, and two days later, more than 65 thousand tweets were posted in which Ukraine was blamed for the disaster that occurred (Muradov, 2020).

Two types of activities were particularly characteristic in cyberspace - posting some content and disabling websites by *DDoS* attacks during which servers are flooded and congested, making them inaccessible to users. Russia has a lot of active hacker groups, such as *Sandworm*, *Cyber-Berkut*, *Sprut*, etc. It is assumed that the Russian intelligence services are ”behind” their activities and operations. Moreover, in 2014, Ukraine organized its cyber groups such as *Falconsflame*, *Trinity*, *Ruh8* and *Cyberhunta* (Pashkov, 2016).

The aim of Russian cyber attacks was to cause an interruption in the Ukrainian power supply system in 2015, which had a great effect on the population. For the first time, cyber weapons has caused major disruptions to civilian infrastructure. The Russian attack in 2016 led to a blackout due to compromising the high-voltage transmission network in Ukraine, which supplies electricity to consumers. The destruction of critical energy and network infrastructure was not the ultimate goal of the Russian attacks. Their purpose was to achieve the greater goals of economic

and political weakening of the state (Stockton, 2021). Russia tried to demoralize Ukrainian troops and Ukrainian population. Using its intelligence capabilities, the Russian military compromised computer networks and sent targeted messages to Ukrainian troops and their families. It also conducted cyber operations in order to disrupt the Ukrainian government and business activities and intimidate Ukrainians and those who might support Ukraine or do business in it (Angevine et al., 2019).

The information infrastructure of Ukraine's *Boryspil* Airport suffered an attack in 2016. The great *online* sabotage against Ukraine's financial and banking sector was further evidence of the Russian cyber attack on Ukraine. On December 6, 2016, a hacker attack disabled the *web*sites of the State Treasury, the Ministry of Finance and the Pension System. After the mentioned events, the attacks on the *web*sites of the Ukrainian Railways and the Ministry of Defence continued. According to Turchynov, Secretary of the National Security and Defence Council of Ukraine, the attacks were pre-planned and coordinated from a centre located in the Russian Federation (Pashkov, 2016).

The course of events in Crimea was shrouded in a sophisticated effort to control the flow of information. Russian information activities encompassed a spectrum of activities in various domains. The former head of the Ukrainian Security Service Valentyn Nalyvaichenko stated that the mobile communications of Ukrainian government officials were compromised. The Government websites and news portals suffered distributed denial-of-service attacks, so-called *DDoS* attacks. All of this contributed to the significant success of the Russian party in the domain of information in Eastern Ukraine. Owing to the internet and social media, the audience was global and communication took place in real time (Jaitner, 2015).

Russia has conducted sophisticated information operations in order to disrupt decision-making and discourage Ukraine from seeking assistance from Western countries. The analysis of the Russian operations in Crimea carried out by NATO emphasizes that Russia was fully prepared to wage information warfare in Ukraine (Stockton, 2021). Messages were prepared and distributed to different parts of the world. New channels of communication were launched, in which the evaluation of the effectiveness of the influence and its appropriate modification, i.e. the change of the narrative in accordance with the current conditions, was conducted. Among all key narratives, in the period from 2014 to 2015, the ”civil war” narrative dominated on the Russian television, after which Ukraine was often referred to as a ”Western puppet” and a ”non-state under external control”. At the same time, Russian literature, newspapers, television and film were popularized in Ukraine.

In Crimea and the Donbass region, it was not possible to obtain information from sources other than local Russian-controlled channels. Ukrainian TV channels were banned. New news channels like *LifeNews* were established, which first started as online news portals, but later grew into influential TV channels. The Russian media giants, *Russia Today* and *Sputnik*, have been actively broadcast in Europe, even in the US. Information operations were flexible, constantly evolving and quickly adapting. A combination of powerful fear mongering has facilitated the successful Russian information war in the Russian-controlled areas of Crimea and Donbass.

Intensive information campaigns promoted among the population enabled the quick and painless Russian takeover of Crimea (Holger and Sazonov, 2018). Some Russian sources stated that Western countries are also waging information warfare against Russia with the aim of discrediting the Russian political regime, weakening its position in the international community and spreading Russophobia.

In the period before the beginning of the armed conflict, Russia had an absolute advantage over the Ukrainian information space, electronic and print media. It has been shown that the presence of the ”fifth column” in the Ukrainian media system, authorities, public organizations and political parties is a very important factor. Russia actively participated in its informational expansion by exploiting the pro-Russian sentiments of a great part of the population in the eastern part of Ukraine. The absence of a language barrier, the mental similarity of the citizens of both states, common history, the closeness of national cultures, a huge network of family contacts, etc., contributed greatly to media activity. Ukraine has adopted certain security measures to counter Russian activities in information space. Namely, in December 2014, the Ministry of Information Policy was established, and later, in October 2015, the International Broadcasting Multimedia Platform of Ukraine was launched. From 2015 until 2016, Ukraine introduced a package of sanctions against the Russian media, journalists, artists, publishing houses, etc. The Ukrainian government cancelled the intergovernmental agreement with Russia on cooperation in the field of television and radio broadcasting in 2014-2016. The National Radio and TV Council banned rebroadcasting of 78 Russian TV channels, and the Ukrainian State Film Agency banned 500 Russian films and TV series broadcast on television or in cinemas (Pashkov, 2016).

The number of *Twitter* accounts spreading pro-Russian information increased dramatically in December and early January 2022 compared to November 2021. Between December 1, 2021 and January 5, 2022, *Mithos Labs* identified 697 accounts spreading pro-Russian content in Ukraine, in comparison to only 58 such accounts identified in November 2021. Moreover, the number of new accounts identified each week steadily increased throughout December and early January 2022. The number of the tweets related to Ukraine and spreading pro-Russian information in December also increased by 375% compared to November and by 3,270% compared to September 2021. Unlike the earlier period, most accounts distribute (mis)information in English, not in Russian. They primarily tried to undermine support for Ukraine in the West (Labs, 2022). On January 15, 2022, *Microsoft* published information about the appearance of the malware called WhisperGate on the systems of the government agencies. Dozens of systems at two government agencies in Ukraine were compromised by a destructive tool that Ukraine believes was a part of a coordinated attack on their computer systems (Microsoft, 2022).

UCMC, StopFake and *Ukraine Today* were three very different platforms related to media production in various ways. Formally, *UCMC* is set up to serve media correspondents, *StopFake* to monitor news, while *Ukraine Today* is organized as a traditional media platform, producing and distributing television content. This implies that the three platforms differ in terms of organization, competence, work methods, strategy, ethics, economic resources and much more. However, all three organizations share a

common goal: to provide the international public with information about the current conflicts in Ukraine-Russia relationship, from a distinctly Ukrainian perspective (Bolin et al., 2016).

The influence of unmanned platforms was very pronounced in that period. The increased volume and intensity of various intelligence and reconnaissance platforms was noticeable. The Russian methods of action in certain segments of information warfare capabilities were revealed in exercises such as ”West-2021” in Belarus and ”Caucasus 2020” near Volgograd, as well as battles in the Donbass region. These findings enabled Ukraine to protect itself, to a certain extent, from the actions of the Russian party. In October 2016, the International Information Consortium ”Bastion” was founded under the auspices of the National Security and Defence Council of Ukraine, whose task was to counter Russian information influence (Pashkov, 2016). Regardless of the above-mentioned, Ukrainian countermeasures were mostly situational, specific to certain sectors and could not fully correspond to the scale of Russian action.

Conclusion

Information war as a hybrid threat is becoming an increasingly serious and sophisticated form of security threat. It manifests itself in different forms, and the consequences for society and state as a whole are increasingly serious. The examples of the Russian information activities, both before and during the current armed conflict in Ukraine, are indisputable. Different forms of information warfare have been implemented, above all cyber, psychological and propaganda action. The Russian information warfare in Ukraine is characterized by a high level of sophistication, integration of various resources, dynamism and flexibility of their use. Some attacks were highly destructive, targeting the Ukrainian critical information infrastructure. The general conclusions, that is, the lessons learned regarding information operations in Ukraine indicate that Russia has prepared for a long time and was very effective, while Ukraine, on the other hand, was quite unprepared for this form of warfare. Information warfare will obviously continue to be a manner of confrontation between Russia and Ukraine in the future, and most certainly as long as combat operations last.

Various conflicts in the post-Soviet space, especially the current ones between Russia and Ukraine, in certain segments resemble the conflicts that took place in the territory of the former Yugoslavia. It can be expected that the process of reconciliation will have many similarities and will be accompanied by many difficulties. Analysing possible models of reconciliation between the states and nations of the former Yugoslavia, it has been noticed that ”political will is a *conditio sine qua non* for the process of reconciliation” (Vučinić, Milenković and Pavlović, 2019: 1001-1102). Without it, it is impossible to persevere in this long and demanding process, which cannot be spontaneous, but has to be managed. The role of modern technology, media and social networks is invaluable in such an undertaking. In this process, activities characteristic of information warfare would have to take place in the opposite direction in order to build trust through (re)affirmation of positive values, narratives and bright examples from the common past.

Literature

1. Angevine, R., Lead, T., Warden, J., Keller, R. and Frye, C. (2019). Learning Lessons from the Ukraine Conflict, Institute for Defense Analyses, Alexandria – Virginia.

2. Bolin, G., Jordan, P. and Ståhlberg, P. From Nation Branding to Information Warfare: Management of Information in the Ukraine-Russia Conflict, ttps://www.academia.edu/28548429/From_Nation_Branding_to_Information_Warfare_Management_of_Information_in_the_Ukraine_Russia_Conflict (22.4.2023.)

3. Constantin S. (2022). *Ethnic and linguistic identity in Ukraine? It's complicated,* https://www.eurac.edu/en/blogs/mobile-people-and-diverse-societies/ethnic-and-linguistic-identity-in-ukraine-it-s-complicated (20.6.2023.)

4. Field Manual No. 3-0 Operations (FM 3-0). https://cyberwar.nl/d/20171005_US-Army-Field-Manual-FM-3-0-Operations.pdf (22.4.2023.)

5. Helmus, T., Bodine-Baron, E., Radin, A., Magnuson, M., Mendelsohn, J., Marcellino, W., Bega, A. and Winkelman, Z. (2018). Russian Social Media Influence - Understanding Russian Propaganda in Eastern Europe, RAND Corporation, Santa Monica - California.

6. Hofman., F.,G., (2007). *Conflict in the 21st Century-The Rise of Hibrid Wars*, Potomac Institute for Policy Studies.

7. Holger, M. and Sazonov, V. (2018). Information Warfare as the Hobbesian Concept of Modern Times - The Principles, Techniques, and Tools of Russian Information Operations in the Donbass, The Journal of Slavic Military Studies, Vol. 31, No. 3, 308-328.

8. Iasiello, E. (2017). Russia's Improved Information Operations: From Georgia to Crimea. Parameters, Vol. 47, No. 2, 51-63.

9. Jaitner, M. (2015). Russian Information Warfare: Lessons from Ukraine, Chapter 10 in Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO Cooperative Cyber Defence Centre of Excellence, Tallinn.

10. Jović-Lazić A. (2015). *Odnosi između Evropske unije i Ruske Federacije: kraj XX i početak XXI veka*, IMPP, Beograd.

11. Jović-Lazić A., Lađevac I. (2018). „Razvoj i posledice ukrajinske krize." Međunarodna politika, Vol. LXIX, No 1172. 27–51.

12. Kofman, M., Rojansky, M., (2015). A Closer look at Russia's "Hybrid War", *Woodrow Wilson International Center for Scholars*, Kennan Cable No. 7.

13. Microsoft. (2022). Destructive malware targeting Ukrainian organizations, https://www.microsoft.com/en-us/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (22.4.2023.)

14. Muradov, I., (2020). Information War in Ukraine Before and After the Donbas Conflict. International Journal of Russian Studies, No. 9/2, 202-222.

15. Mythos Labs. (2022). Analyzing Twitter Disinformation/Propaganda Related to Russian Aggression Against Ukraine - Report Number 4, https://mythoslabs.org/wp-content/uploads/2022/06/Part-IV-Analyzing-Pro-Russian-DisinformationPropaganda-Related-to-Ukraine.pdf (22.4.2023.)

16. *NATO recognises Ukraine as Enhanced Opportunities Partner,* https://www.nato.int/cps/en/natohq/news_176327.htm (30.6.2023.).

17. NATO Strategic Communications Centre of Excellence, Russian information campaign against Ukrainian state and defence forces, https://stratcomcoe.org/publications/russian-information-campaign-against-ukrainian-state-and-defence-forces/174, (22.4.2023.)

18. Pashkov, M. (2016). Russiaa's Information Expansions: Ukranian foothold, https://razumkov.org.ua/uploads/article/2017_Information_Warfare.pdf (22.4.2023.)

19. Pierzchała, K. (2019). Information Warfare Between Russia and Ukraine: A Cause of War for the West?, Polish Political Science Yearbook, Vol. 48, No. 1, 103-111.

20. Robert, S. (2016). Framing of the Ukraine-Russia Conflict in Online and Social Media, NATO Strategic Communications Centre of Excellence, Riga. https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf (22.4.2023.)

21. Samardžić N. (2021). *Drugi hladni rat: Zapad i Rusija 1999-2019*, Laguna, Beograd.

22. Stockton, P. (2022). Defeating coercive information operations in future crises. The Johns Hopkins University Applied Physics Laboratory, Santa Fe – New Mexico.

23. Unwala, A. and Ghori, S. (2015). Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict. Military Cyber Affairs, Vol. 1, No. 1, 1-11.

24. Vučinić D., Milenković M., Pavlović K. (2021). Reconciliation in South Africa as a(n) (Im)possible Model for the Post-Yugoslav Area, *Teme*, Vol. XLV, No 3, 987-1004.

25. Vuletić, D. i Đordjevic, B. (2021). Problemi i izazovi upravljanja internetom na medjunarodnom nivou", *Međunarodni problemi*, Vol. LXXIII, No. 2, 235-258.

26. Vuletić, D. i Đordjevic, B. (2022). Rivalstvo Sjedinjenih Američkih Država i Rusije u sajber prostoru. *Međunarodni problemi*, Vol. LXXIV, No. 1, 51-74.

27. Vuletić, D., Stanojević, P. (2022). Concepts of information warfare (operations) of the United States of America, China and Russia. The Review of International Affairs, Vol. LXXIII, No. 1185, 51-71.

28. Walker N., (2023). *Conflict in Ukraine: A timeline (2014 – present)*, The House of Commons Library, London.

29. Миленковић М., Митровић М., (2019). Обојене револуције у парадигми хибридног рата, *Војно дело*, Vol. 71, br. 6, str. 248-263.

30. Миленковић М., Суботић М., (2017). Насилни недржавни актери и позиција Србије, *Српска политичка мисао*, Год. 24. Vol. 57. No. 3, 55-70.

31. Митровић М., Николић Н. (2022). *Хибридни рат: допринос дефинисању концепта, садржаја и модела деловања*, МЦ „Одбрана", Београд.

32. *Путиново обраћање пред специјалну операцију у Донбасу – Интегрално*, Портал Спутњик, (2022) https://sputnikportal.rs/20220224/putin-cilj-vojne-operacije-u-donbasu---zastita-ljudi--1134704633.html (30.06.2023.)

33. *Стратегія національної безпеки України (2020)*, https://zakon.rada.gov.ua/laws/show/392/2020#n2 (30.06.2023.)