ELECTRONIC WARFARE - LESSONS LEARNED FROM RUSSIA'S ATTACK ON UKRAINE

Captain (N) (ret.) Professor Sorin TOPOR, Ph.D*

Abstract*: Hybrid conflicts are becoming more frequent and surprising. It is increasingly difficult to try to do a forecast for future military operations. Analysing the beginning of Russia's special military operation, at one year, we can see that, from one stage to another, the strategies, forms and action methods are extremely diversified by introducing new technologies and tactics. In this paper we intend to establish the place and role of the electronic warfare in this conflict and to establish some landmarks for the reform of the conception of development of the electronic warfare in the Romanian Army.*

Keywords*: Electronic warfare, war in Ukraine, Russia's special military operation.*

Introduction

One year after the debut of Russia's special military operation on Ukraine we intend to analyse the place and role of electronic warfare within the Hybrid War conception carried out by Russia on Ukraine. The results obtained are landmarks for the modernization of forces and for the estimation of hypothetical models for defense of our country.

As it is known, Russia has always attached great importance to electronic warfare. In his approaches about the "war of the new generation" the electronic war is characterized by a series of new systems and innovative tactics, in close relationship with the development of UAV systems, massed fires with advanced warheads and sub-munitions, reform of the major tactical units in combat groups, mobile and combined, such as mobile brigades of combined weapons, air assault and special operations brigades, mobile and advanced anti-aircraft defense units etc. A combat team is capable to conduct of decisive action in combined operations, with kinetic and cyber strokes.

Until the outbreak of special military operation, Russia has developed sophisticated electronic warfare elements that integrate

* National Institute for Research and Development in Informatics - ICI Bucharest, associate member of the Academy of Romanian Scientists, sorin.topor@ici.ro

technologies and applications for electronic war, for the entire spectrum of the information and cyber warfare. The defense industry has presented remarkable scientific achievements and technologies that have allowed existing equipment upgrades and creating new combat systems to support the armed forces action.

Last but not least, Russia's participation in missions from various war theatre such as Syria, Georgia, Ukraine (2014), but also in military exercises with external partners (usually with Belarus) allowed Russian armed forces to test the new equipment, to study and to identify new tactics for their use.

Experimental details

We present the most relevant sequences that characterize the electronic warfare operations carried out between February 2022 - February 2023. By far, it is observed that both actors involved have used aerial drones of various types and sizes, civil and military, for the purpose of collecting information, monitoring the maneuvers of ground forces and the fire targeting. It can be considered a war of drones.

The Russian electronic warfare tactics analysis

The beginning of the Russian invasion (24.02.2022) was preceded by powerful jamming and electronic misinformation. In the first phase of the war, Russia granted a low interest to the Ukrainian electronic warfare capacities knowing the combat capabilities, most of systems being made in Russia. The technological differences come from the fact that Russia, after the 2008 financial crisis, has continued its strategy for the development and modernization of all the battle capabilities. Ukraine focused on other objectives that he considered priority at national level. After 2013, Russia implemented extensive reforms and upgrades within the armed forces from the western part of the country, and after 2014 it created three armies [1]. They were equipped with modern combat systems, in particular, for CBRN defense, special operations, electronic warfare, armoured vehicles and JISR.

Although the budget allocated to the defense was quite small compared to other NATO states, Russia has managed to implement new

[1] Muzyka, K. (2021), *Russian Forces in the Western military District*, the CNA Occasional Paper, available at https://www.researchgate.net/publication/350313637_Russian_Forces-_in_the_Western_Military_District accessed at 18.01.2023.

concepts of development, coordination and stimulation of the defense industry capabilities to position themselves quite well compared to most European states and to endure well the effects of Covid 19 disease.

Above to the beginning of the war, the first measures based on "Gherasimov's doctrine " were implemented within the Russian armed forces. General Valeri Gherasimov, the head of the General Staff, drew attention to a speech from 2013 at the General Staff Academy that there are "forms and methods of asymmetrical operations ... which make it possible to level an enemy in an armed fight"[2] referring to information tactics. Gherasimov estimated that a cyber corp will be set up in 2013, army information forces in 2017 and the Foundation for Advanced Research (the equivalent of US's Defense Advanced Research Projects Agency). There is no information about the existence of these new structures. Selhorst's analysis of Russia's perception of the concept of war, based on lessons learned in Estonia and Georgia, applied in Ukraine (2014), presents the importance of convergence between the cyber and electronic warfare[3], without directly nominating them.

In an analysis regarding the implementation of the Gherasimov's doctrine within the Russian armed forces lt.col. Timothy Thomas[4], emphasized that the new vision of the war brings deep changes in content and not in the form of military operations. The quality of the warfare will be determined by the quality of the armament and the methods of employing them. A quality warfare must include the fire shoots, electronic warfare, robotic, aerospace, air mobility, air assault, intelligence-reconnaissance warfare, counterintelligence operations and other, in which the combat and non-combat maneuvers converge. The Russian operations will be characterized by indirect effects, without direct contact and with active preventive strikes. The Russian conception establishes that electronic warfare is part of the Anti-Acces/Area Denial (A2/AD) strategy adapted to

[2] Gherasimov, V. (translated by Dr. Harold Orenstein), *Thoughts on Future Military Conflict – March 2018*, available at https://www.armyupress.army.mil/Portals/7/Army-Press-Online-Journal/documents/2019/Gerasimov-2019.pdf accesed at 12.01.2023.

[3] Shelhorst A.J.C. (2016), *Russia's Perception Warfare*, Militaire spectator, available at https://militairespectator.nl/artikelen/russias-perception-warfare, accessed at 12.02.2023.

[4] Thomas, T., *Russian Forecasts of Future War*, in Military Review (May-June 2019), available at https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/, accessed at 22.02.2023.

combat NATO C4ISR systems. Electronic warfare is an integral part of kinetic and non-kinetic operations carried out both in forces support and by independent management[5].

In the first phase of the invasion, much of the electronic warfare systems were on airplanes to ensure a concentration of the electronic effort on the targets from the depth of the Ukrainian territory and to support the action of the ground forces. A major problem of the excessive use of the electronic attack has led to the fratricidal jamming in numerous fighting sectors. The emitted jamming signal cannot discriminate the target enemy receiver from the own and friend forces. Noting that the Ukrainian anti-aircraft defense system was still operative after the massive Russian electronic attack and the risk of fratricidal jamming forced the Russians to very careful planning, organization and control of the electronic hits over the Ukrainian systems. Subsequently, the electronic attacks were performed in areas focused on distinct missions on air-air and ground-air communications, as well as on radar and navigation systems.

Another problem was determined by the logistics support in relation to the dislocation of forces. The initial combat positions respect the hierarchical organization of forces. The problems occurred when the logistics flows had excessive delays in insurance with equipment, fuel, ammunition and foods for troops. By default, during the reorganization maneuvers of the combat positions and the electronic war units were influenced.

In the second phase of the invasion, Russia changed their offensive organization on combat alignments and combined the equipment of the strategic and tactical levels.

From the point of view of the electronic warfare they organized the following alignments:

1) The first alignment, about 1 - 3 km from the contact line, were made up of electronic tactical mobile or portable systems, combined with SIGINT equipment. With the Benthos, Mercury-BM, Lille-2, Roland-Jet-Ad etc. systems have performed interception, localization and blocking adversary communications in VHF and GSM.

[5] Thomas T. (2018), *Russia's Forms and Methods of Military Operations, The Implementers of Concep*t, available at https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2018/Russias-Forms-and-Methods-of-Military-Operations/, accessed at 20.01.2023.

2) The second alignment, about 15-30 km from the contact alignment, consisted of the Lille-3, Re ident, R-943UM, Borisogrebsk-2 equipment with the mission to intercept the opponent's radio communications and produce jamming, misinformation and misleading.

3) The third alignment was disposed of at 60-240 km consisting of equipment of Moscow-1 and Krasuha-4 with missions to ensure electronic support, surveillance and suppression of the adversary electromagnetic interference.

4) The strategic equipment such as Murmansk-BN and Auto Yard were much in depth on the Russia territory and ensured the monitoring of strategic radio traffic, especially the strategic communications of Ukraine with various NATO components. These combat positions being fixed or slightly movable performed active jamming missions only at critical moments, when they considered that the set limits were violated, such as NATO air raids over the state border.

This reorganization allowed:

- Optimizing control over the command and control system (C2) of the Ukrainian forces out of contact. For example, the radio jam in the Dombass region has completely blocking radio communications. Usually, for this task were intended for Borisogrebsk-2, R-300KMW and Boris Glebsk-2 systems. Interestingly, the Russians also used previously used equipment. The Radio R-1330ZH radio jams have been used against the Ukrainian cruise-missile receivers' jammer, artillery fire system directed by radio wave, UAV systems and other radio stations in brigadier tactical units.

- Navigation jams on GPS systems. Prior to the start of the special military operation, Russia carried out GPS jamming on a large scale, along the Ukrainian-Belaruse border, north of Chernobyl, as well as in the Dombass region. For this he used the Shipovnik-Aero system, which launches false navigation signals for the misleading of navigation radars, radar of air targeting systems, and radars of missile management systems. In addition, Russia has launched GPS jams on the geographical areas of Crimea/Black Sea and the Baltic Sea to disturb the freedom of movement of NATO recognition and surveillance aircrafts.

- The jamming attempts of satellite links with the Tianye-21 system and other equipment installed on pillars and communication antennas

- The jamming against the radars of the Ukrainian anti-aircraft defense systems has greatly supported the air forces missions during the air strikes. The Beech, Viespa and Khibiny jamming aircraft systems can automatically detect and block the radar of the anti-aircraft defense system. But can also block the radar of a friend airplane if it operated in the same frequency spectrum.

Other electronic warfare executed during SEAD missions have involved anti-radiation missiles that have taken over numerous Ukrainian early warning radars and missile launching installations. Only on June 13, 2022, 338 Ukrainian anti-aircraft installations were destroyed with KH-31 missiles launched from Su-35 aircraft.

- The Russians electronic disinformation had two objectives: 1) misinformation of the striking vectors and their control systems; and 2) disinformation of personnel. Numerous types of active and passive countermeasure chaff and electronic decoys, air or land deception maneuvers, as well as some active jamming actions, were used to misinform the targeting systems. The Krasuha-4 generated false targets for the radar of the Ukraine and NATO anti-aircraft defense system. The efficiency of the jamming was quite good causing Ukrainian forces to launch numerous electronic attacks and physical response, which caused the revealing the forces position and, subsequently, their attack.

- Jamming on the emissions of the national mass-media radio stations. Even though the equipment had protection systems against various types of interference Russian specialists hack these and perform jamming on relevant emissions.

- GSM monitoring and jamming. The intermittent radio jam tactics allowed the Russians to concentrate the monitoring of communications through GSM in space and time. The Ukrainian troops who kept in touch with families or civilians who used mobile phones could only speak when the GSM monitoring was possible. Much information about the Ukrainian army and their maneuvers were obtained from the services of social networks. With Lille-3 the Russians sent numerous text messages to the Ukrainian mobile phones to convince them to surrender and to weaken the morale of the troops. In addition, the GSM mobile phone area became target for artillery fire

Regarding the electronic defense of the Russian forces, a great vulnerability was the limited holding radio with protected systems and the

use and by the Russian military of the GSM civilian mobile phones. Observing this, from the first phase of the special operation, the Russians have limited the use of social services by imposing a very strict radio discipline. The analysis of the streams video on the Internet, related to the battle space, demonstrates that only the Ukrainians and, sometimes, the Chechen forces, posted moving and images.

In this military operation, the Russians created a new utility to the electronic war, the jam being involved in combating Ukrainian drones. With Krasuha systems struck the sensors and the drone control system, which led to premature wear and/or down. Radio jamming produces GPS receptor blocking or fake target induction that prevents the drone from identifying the normal route. Last but not least, the radar altimeter jamming will be bumped by leaving the air security area and exposing it to combat with Armor, Pishchal-PRO, Taran-PRO, Sapsan-Bekas, Luch and Kupol. The extremely large number of drones consumed demonstrates the efficiency of the jamming. Only on June 20, 2022, 1260 Ukrainian drones were shot down by the Russian army. Numerous wrecks found on the ground had no traces of bullets or burns were obviously out of control through radio jamming

Critical analysis of the Ukrainian army electronic warfare

From the point of view of the capability of the Ukrainian army with electronic warfare equipment, we appreciate that Ukraine no longer has functional systems, those held quickly detected and neutralized by the Russian army.

Ukrainians jam the Russian communications radio by overlapping their own radio emissions over those of Russian communications links. For information and electronic defense they used their own interception and location systems, as well as the support of information from NATO, especially for the monitoring of Russian electronic attack systems.

For the Ukrainian force protection, the principle of decentralization of the command and control (C2) rapidly implemented against the total radio jam executed by the Russians. The biggest vulnerability of this strategy was the decrease of the fighter's morale, located in decentralized combat positions, due to the lack of information. In the beginning, the Ukrainian and Western mass-media deliberately decreased the number of information about the real maneuvers and the evolution of war, in some

situations accusing the Russian army of not electronic warfare effects. In order to stimulate the Ukrainian will to fight of population, a series of programs were broadcast by which the fighters were not surrender. However, due to the overwhelming number of electronic attacks executed by the Russians, the way of government communicating with its citizens had to be modified. On March 6, 2022, the Minister of Defense of Ukraine, Oleksii Reznikov, asked the people to seek and destroy the Russian electronic warfare and intelligence equipment. He said that *"the task of all citizens who care about it (our army a.n.) is to destroy the supply columns and EW systems ... This will significantly weaken the Russian troops and offer an advantage to our soldiers. The occupants will become powerless"*[6]. After this moment, more and more images with Russian electronic warfare equipment began to appear in the press, broken or destroyed, with extensive references to the way they were captured by the Ukrainians.

Some of the few successful actions belonging to the Ukrainian electronic warfare are related to the exploitation of a great vulnerability of Russian aircraft. These, in the face of the heat-seeking missile attack cannot respond with flares as electronic protection measure. Most Russian aircraft are easy targets for the Stinger, 9K38 Needle and other NATO air-air missiles.

Another tactic of the Ukrainian forces was high mobility of the combat forces under the effect of electromagnetic silence. The quick removal from the effect of direct strike produced quite large losses but in a much time than the Russian army had planned. Moreover, the communications systems of the special forces penetrated into the depth of the Russian defense used only encrypted lines and only at critical moments. The equipment made available by NATO are the latest. Ukrainian forces have access and began to use the NATO Single Channel Ground and Airborne Radio System (SINCGARS)[7].

In the radar field, the Ukrainians were very attentive to organizing and carrying out the combat positions in relation to the amount of masking

[6] Radio Svoboda, *Міністр оборони закликав українців знищувати російські системи радіоелектронної боротьби і розвідки*, available at https://www.radiosvoboda-.org/a/news-inistr-oborony-reznikov-ukraintsi/31745048.html, accessed at 20.02.2023.

[7] Clark, B., *The Fall and Rise of Russian Electronic Warfare*, IEEE Spectrum, available at https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare, accessed at 22.02.2023

resources for camouflage and electronic disinformation. However, the losses were considerable. Only on the first day of battle they lost 36 radars, 13 control stations and radio stations, as well as 14 anti-aircraft launcher systems. However, the limited use of radar and radio jamming only at critical moments was an extremely effective measure that was confirmed by Russian failed attempts to try key urban settlements in northern Ukraine, such as Kiev or Harkiv. The measures of Ukrainian forces, cumulative with a number of factors such as the Russian limited logistics with fuel, ammunition and provisions, together with a difficult ground access have stopped advance of Russian armoured columns in several key directions, making useless the Russian electronic attacks in all the electromagnetic spectrum.

Regarding the support of Ukraine by NATO with systems and technologies for the defense we notice that Ukrainian forces have begun to resist when they received encrypted communications equipment from USA and Turkey.

Regarding the making available of electronic war equipment, no country gives details.

Last but not least, the Starlink service offered by Elon Musk provides undeniable support for Ukraine. Musk's concern about increasing the efforts of the Russians to jam the satellite communications links has led him to warn the Ukrainians that they should hold terminals stopped when possible because they are vulnerable to geolocalization and can be milestones for fire planning.

Other observations about electronic warfare in this war

Russia is capable of integrating the capabilities of electronic and cyber warfare at all hierarchical, tactical, operational and strategic levels. Russia has numerous electronic warfare systems, capability and know-how in the field.

At the strategic and operational level, Russia has five electronic war brigades, two of them in the Western Military District[8]. At the Navy there are five electronic war centres (brigadier level), three for the European

[8] Spring-Glace, M., *Return of Ground-base Electronic Warfare Platforms and Force Structure*, in Military Review (July-August 2019), available at https://www.armyupress-.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2019/Spring-Glace-Electronic-Warfare/, accessed at 22.02.2023.

fleets and two for the fleet of the Pacific Ocean[9]. The Russian Aerospace Forces have independent electronic warfare battalions (equivalent to the EW brigades of Ground Forces) in at least four of the five air and anti-aircraft defense armies. They are adapted to operate with the EW brigades of ground forces.

Each EW brigade consists of four EW battalions that can carry out operative and strategic missions or support the activity of tactical-operative units of ground forces. They have: the complexes RL257 Krasukha-4, L260 Krasukha-2, Murmansk-BN, Borisoglebsk-2, RB-341V Leer-3, Svet-KU, Infauna, Lesocek, Jitel, Dziudoist, Zaslon-REB and many more[10].

This equipment can be used independently or conjugated with others. In Syria, a Krasukha-4 system has operated with the TK-25 shipborne electronic countermeasures system for intercept and blocking signals from airborne and shipborne target acquisition radar systems, as well as against anti-ship missiles[11]. The first system detects the target and the second suppress the activity of the radar.

The RB-341V Leer-3 system can extend its range by using an Orlan-10 (UAV). With these systems, the tracking of mobile phone users, the distribution of fake text messages to network users and targeting for the artillery fire are carried out.

The maneuver enhancement brigades are equipped with an electronic warfare company, an unmanned aerial systems (UAV) company, and an intelligence support platoon. Within an electronic warfare company are 12 mobile platforms and 15 portable systems. For VHF radio jamming the Russians mainly used R-934B and SPR-2 VHF/UHF. For HF radio jamming, EW companies have Murmansk-BN, Pole-21 or R-330H Zhitel[12]

---

[9] Copcea I., *Războiul electronic devine componentă esențială în doctrina pentru operații a Forțelor Navale ruse*, Desense Romania, available at https://www.defenseromania.-ro/razboiul-electronic-devine-componenta-esentiala-in-doctrina-pentru-operatii-a-fortelor-navale-ruse_606497.html accessed at 21.02.2023.

[10] Tass, *Чем армия России может "ослепить" и "подавить" противника*, available at https://tass.ru/armiya-i-opk/6328905, accessed at 22.02.2023.

[11] Cranny-Evans, S., *Fields of silence and broke cycles: Russia's electronic warfare*, in Global Defence Technology, available at https://defence.nridigital.com/global_defence_-technology_mar22/russia_electronic_warfare, accessed at 22.02.2023.

[12] Pravda, *Nurmansk-BN systems turn F-35 figters into scarp metal near Russian borders*, available at https://english.pravda.ru/news/world/149839-murmansk_f_35/, accessed at 21.02.2023.

systems. They operate on radio communications between aircraft, ships and satellites in order to degrade the accuracy of radio and GPS guided weaponry.

By combining actions in the cyber and information environments, ground structures have as their main missions the protection of operational level structures and the denial of air enemy access, by integrating air defense capabilities as part of the A2/AD strategy.

Before the war, Russian military strategists tested various tactics in war (Georgia and Syria) or peace time. The event involving the American destroyer USS Donald Cook when it entered the waters of the Black Sea to carry out a routine patrol mission is a good example. On 04/15/2014, a Russian Su 24 flew over the USS Donald Cook and performed several passes simulating the ship's attack. The problem arose when it was found that the Russian Khibiny airborne system was able to shut down all electronic systems on ship board, including those belonging to the Aegis system[13].

Russian GPS jamming equipment led to the inclusion of anti-jamming algorithms in NATO GPS navigation systems and their adaptation to the inertial guidance regime as a secondary system. In Syria, numerous NATO strike vectors equipped with precision guidance systems have been disrupted, which has produced an increased ammunition consumption and, at the same time, a decrease in the effects of some missile strikes.

Regardless of the number of drones' losses, they were the most intensively used. Both Ukrainians and Russians use small arms, machine guns, portable anti-aircraft missiles and electronic jamming to shoot down them[14] and cyber-attacks[15] to gain control over their operation. Officials from both forces involved acknowledged that there are areas where the drones could not be used because the adversary uses radio jamming on GPS systems and their control radio links. The Russian Rosehip-AERO anti-

[13] Sharman, J., *Russia claims to have weapon that could cripple the US Navy, State new report surfaces three years after alleged o jammer against American destroyer*, available at https://www.independent.co.uk/news/world/europe/russia-weapon-us-navy-cripple-electronic-signals-deactivate-defence-systems-a7693816.html, accessed at 16.01.2023.

[14] BBC, *How are kamikaze ‚drones' being uded by Russia and Ukraine?* available at https://www.bbc.com/news/world-.62225830, accessed at 17.02.2023.

[15] Burridge, T.S., *Inside Ukraine's critical drone warfare campaign against Russia*, available at https://abcnews.go.com/International/inside-ukraines-counteroffensive-drone-warfare-small-group-hackers/story?id=91104098, accessed at 18.02.2023

drone system is an electronic warfare equipment that replaces jamming errors with dynamic navigation space coordinates forcing the drone to land at the location determined by the electronic warfare system.

Space 's Starlink low-orbit satellite Internet service allowed the Ukrainian military to use broadband communications and Internet services, according to the agreements. And other commercial companies have provided satellite services to Ukraine for monitoring districts and force maneuvers, for monitoring refugee flows etc. Among them we mention OneWeb, Planet and MDA. When the Ukrainians used the Starlink service to control drones[16], Russia tried to jam the Starlink signals by making temporary blackouts. For this they used the Suha-2, Krasuha-4 and Jilada-2 systems.

Also, the Russian army uses specialized Il-22PP electronic warfare aircraft, in strategic and operational missions, for the electronic suppression of land, air, sea and space targets. There is information that they would also use the Mi-8MTRP-1 Rychag helicopter, specialized in electronic suppression of air defense systems[17].

Results

We appreciate that the analysed period is characterized by the following innovative approaches and new electromagnetic vulnerabilities of combat systems:

1) The fire strikes from a long distance (with artillery or missiles), simultaneously with cyber warfare, satellite support and electronic warfare. The greatest vulnerabilities of the command and control (C2) systems were generated by the poor provision of modern communication equipment. The introduction of mobilized personnel into combat units without going all the stages of military training increases the negative effects. The need to maintain a large reserve of forces and systems adapted to operations in the

[16] Coșlea A., *„Trebuie să alegeți o tabără”.Space X interzice Kievului să folosească tehnologia Starlink pentru controlul dronelor*, available at https://www.hotnews.ro/stiri-razboi_ucraina-26073054-trebuie-alegeti-tabara-spacex-interzice-kievului-foloseasca-tehnologia-starlink-pentru-controlul-dronelor.htm accessed at 20.02.2023.

[17] Copcea, I., *Rușii folosesc în Ucraina un model de elicopter extrem de rar-Mi-8MTPR-1 Rychag, specializat în războiul electronic*, Defense Romania, available at https://www-.defenseromania.ro/rusii-folosesc-in-ucraina-un-model-de-elicopter-extrem-de-rar-mi-8mtpr-1-rychag-specializat-in-razboiului-electronic_618745.html accessed at 21.02.2023.

electromagnetic environment and in cyberspace has determined the non-involvement of all specialized units from all military forces.

2) Lack of proper training of radio and radar operators produced fratricidal jamming and disruption of electromagnetic situation knowledge at critical times. On the stress background the operators used too much active jamming.

3) A main advantage of the Russian electronic warfare is determined by its mobility capabilities, with most systems being on tank tracks and wheeled vehicles. The terrain created big problems for electronic warfare units. The scratchy terrain of front lines with many landforms makes it difficult to use electronic warfare without affecting own forces operating in their vicinity. When the Russian forces tried to destroy the antennas of the 3G cellular systems in the Harkiv region, they also disabled the services of their own military cryptophone network because it also operated on 3G/4G technology. Moreover, due to the use of the same type of technology the Russians could not completely disrupt the cyber infrastructure through cyber and kinetic strikes.

Ignorance of electromagnetic vulnerabilities allowed Ukrainian forces to counter the quantitative and technological advantage of the Russian military. Dispersed and highly mobile combat groups conducted harassing attacks on the armored columns that the Russians relied on in their special operation.

4) The delivery of a variety of radio communication systems by several NATO armies to the Ukrainians increased the level of electronic protection of battlegroup communications. In addition, in urban war areas still inhabited by civilians, the Ukrainian military GSM emissions used have make discredited very difficult from military to other civilian phone broadcasts. Information extracted from the command mode of the Krasukha-4 system, captured on the outskirts of Kiev in mid-March 2022, demonstrates the Russian interest and practical limits in solving this issue.

Conclusions

Modern warfare heavily base on the electromagnetic spectrum and cyberspace, and electronic operations are the key to taking advantage of the electromagnetic spectrum. The concept that electronic victory means victory in war is becoming more and more real.

The relative rigidity of the front lines and the use of electronic terrain masking in a combat positions with dispersed and irregular structures will constitute advantages for planning and organization of temporary defenses in the face of an enemy approaching a multi-domain offensive strategy.

The modern equipping and creating an adequate reserve are priority requirements. For this, the training of the operators of the electronic warfare equipment must be done in advance considering the extremely high consumption of forces and means within the conflict. At the same time, national technological production must be established for the fabrication of proprietary equipment to avoid surprise and possible embargo policies of the support states of adversary's action.

In the context of a high-intensity war, electronic warfare capabilities are a threat to the enemy's conventional ISR systems. If we accept that most future wars will be in highly urbanized and digitized environments, electronic warfare systems will be a real support in combating an extremely large number of complex and varied targets, many of which may be hidden among the electronic signatures of civilian infrastructures.

Electronic warfare tactics will continue to bring asymmetric advantages to battlegroups by slowing or confusing enemy forces without causing direct casualties. Modern electronic attack technologies with very high frequency and high-power electromagnetic waves can damage adversary vehicles making them vulnerable to harassment tactics and ambushes.

The convergent electronic and cyber-attacks on adversary logistics and infrastructure elements can slow force maneuvers by disrupting IT networks used to manage supply stocks and warehouse movements. These networks are unlikely to be as strong protected as operational networks. Hitting them would not require high performance tactics such as those related to a troop C2 systems.

In this context, electronic warfare redefines its role as a basic support of the contemporary armed forces and the lessons learned from the analysis of the conflicts between Russia and Ukraine, for the planning and development structures of the armed forces in Romania, must represent a solid fundation for reforms for all categories of forces.

BIBLIOGRAPHY

BBC, *How are kamikaze ‚drones' being used by Russia and Ukraine?* available at https://www.bbc.com/news/world-.62225830;

BURRIDGE, T.S., *Inside Ukraine's critical drone warfare campaign against Russia*, available at https://abcnews.go.com/International/-inside-ukraines-counteroffensive-drone-warfare-small-group-hackers/story?id=91104098;

CLARK, B., *The Fall and Rise of Russian Electronic Warfare*, IEEE Spectrum, available at https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare;

COPCEA I., *Războiul electronic devine componentă esențială în doctrina pentru operații a Forțelor Navale ruse*, Desense Romania, available at https://www.defenseromania.ro/razboiul-electronic-devine-componenta-esentiala-in-doctrina-pentru-operatii-a-fortelor-navale-ruse_606497.html;

COPCEA, I., *Rușii folosesc în Ucraina un model de elicopter extrem de rar-Mi-8MTPR-1 Rychag, specializat în războiul electronic*, Defense Romania, available at https://www.defenseromania.ro/rusii-folosesc-in-ucraina-un-model-de-elicopter-e trem-de-rar-mi-8mtpr-1-rychag-specializat-in-razboiului-electronic_618745.html;

COȘLEA A., *„Trebuie să alegeți o tabără".Space X interzice Kievului să folosească tehnologia Starlink pentru controlul dronelor*, available at https://www.hotnews.ro/stiri-razboi_ucraina-26073054-trebuie-alegeti-tabara-spacex-interzice-kievului-foloseasca-tehnologia-starlink-pentru-controlul-dronelor.htm;

CRANNY-EVANS, S., *Fields of silence and broke cycles: Russia's electronic warfare*, in Global Defence Technology, available at https://defence.nridigital.com/global_defence_technology_mar22/russia_electronic_warfare;

GHERASIMOV, V. (translated by Dr.Harold Orenstein), *Thoughts on Future Military Conflict – March 2018*, available at https://www.-

armyupress.army.mil/Portals/7/Army-Press-Online-Journal/-documents/2019/Gerasimov-2019.pdf;

MUZYKA, K. (2021), *Russian Forces in the Western military District*, the CNA Occasional Paper, available at https://www.researchgate.-net/publication/350313637_Russian_Forces_in_the_Western_Military_District;

Pravda, *Nurmansk-BN systems turn F-35 fighters into scrap metal near Russian borders*, available at https://english.pravda.ru/news/-world/149839-murmansk_f_35/;

Radio Svoboda, *Міністр оборони закликав українців знищувати російські системи радіоелектронної боротьби і розвідки*, available at https://www.radiosvoboda.org/a/news-inistr-oborony-reznikov-ukraintsi/31745048.html;

SHARMAN, J., *Russia claims to have weapon that could cripple the US Navy, State new report surfaces three years after alleged o jammer against American destroyer*, available at https://www.independent.-co.uk/news/world/europe/russia-weapon-us-navy-cripple-electronic-signals-deactivate-defence-systems-a7693816.html,;

SHELHORST A.J.C. (2016), *Russia's Perception Warfare*, Militaire spectator, available at https://militairespectator.nl/artikelen/russias-perception-warfare;

SPRING-GLACE, M., *Return of Ground-base Electronic Warfare Platforms and Force Structure*, in Military Review (July-August 2019), available at https://www.armyupress.army.mil/Journals/-Military-Review/English-Edition-Archives/July-August-2019/Spring-Glace-Electronic-Warfare/;

Tass, *Чем армия России может "ослепить" и "подавить" противника*, available at https://tass.ru/armiya-i-opk/6328905;

THOMAS T. (2018), *Russia's Forms and Methods of Military Operations, The Implementers of Concep*t, available at https://www.armyupress.-army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2018/Russias-Forms-and-Methods-of-Military-Operations/;

THOMAS, T., *Russian Forecasts of Future War*, in Military Review (May-June 2019), available at https://www.armyupress.army.mil/Journals/-Military-Review/English-Edition-Archives/May-June-2019/Thomas-Russian-Forecast/.