MITRE | Center for Technology and National Security

RUSSIA'S ELECTRONIC WARFARE FORCE

BLENDING CONCEPTS WITH CAPABILITIES

by Timothy Thomas

 # 19-2714 9-10-2020

Executive Summary

As the Department of Defense finally begins to appreciate the importance of electronic warfare (EW) on the battlespace against a peer competitor, understanding the conditions US forces should expect in this domain is critical to employing resilient command and control (C2) at all levels. This analysis of Russian leadership thoughts on and recent developments in electromagnetic warfare (EW) — and the recommendations that flow from it — is therefore a needed step in preparing for possible future conflict.

Major General Yuriy Lastochkin, head of Russian Defense Ministry's Radio-Electronic Warfare (REB) force, believes REB capabilities will permit his forces "to decide the fate of all military operations" in the near future. They will be arrayed against what Russia considers a major Western weakness: heavy reliance on continuous, high-bandwidth networks — and in particular space-based assets — for almost every facet of warfare. This raises three particular concerns for U.S. forces and those of their allies and partners.

First, even as the United States and European nations worry about Russian anti-access/area denial (A2AD) strike concepts and capabilities, Russia is prioritizing a EW-based program to cause confusion in "Blue" command and control systems. Concrete steps taken recently include establishing REB as an independent branch, experimenting with REB maneuver units, and focusing on developing a disorganization plan for use in each REB brigade.

Second, Russia appears to be experimenting with this C2 disorder in live engagements, including the attempt to disrupt NATO's Trident Juncture exercise and reported jamming of unmanned vehicles in Syria. Analysis also reveals concepts to protect its Arctic Northern Sea Route through this disorganization while REB units are being integrated with broader deception techniques to create fake targets as part of local exercises. These live engagements and experimentations help turn theory into practice.

Third, Russian system proliferation and development is such that a renewed effort to study and exploit these actual REB systems for their potential tactics and techniques is required. In doing so, they can then be placed into specific functional categories including reconnaissance, jamming, distorting navigational fields, and obtaining lines of bearings for electronic signals sources. Binning these systems into their core functions focuses development and deployment to countering these systems for US and other friendly forces.

For Western analysts, recommendations from this analysis include:

The West needs to stop mirror imaging. There is one Russian refutation after another that they do not spend time conducting hybrid warfare. Instead, it's the West that uses the concept against Russia. Instead, Russia is focused on asymmetric actions and ways to disorganize an opponent, including through the use of EW. Understanding adversarial capabilities and methods that Western practitioners have not considered to date will make their own concepts stronger. This will require close study of Russian REB tactics and techniques to scope out which are new and potentially useful to Western practitioners.

The West must follow and better understand these disorganization concepts as Russia further refines them. While the West worries about Russian A2AD concepts, it is more likely that Russia is putting together a program that will cause chaos in Western control systems through the disorganization of adversary command and control. The Russians are now expanding the use of REB as an independent branch, experimenting with REB maneuver units, and focusing on developing a disorganization plan for use in each REB brigade.

Start watching what theories are blending into real actions during exercises, which will provide better input and expectations from Russian intentions. Russia appears to be experimenting with C2D in live engagements, such as the attempts to disrupt NATO exercises like Trident Juncture. It is training with C2D via systems like Murmansk-BN to protect its Northern Sea Route and access to vital resources there.

Western specialists need to become more aware of how REB could be integrated with deception techniques. This requires an understanding of Russian maskirovka, spoofing, and reflexive control techniques and the equipment (inflatable equipment, fake frequency sources, etc.) developed to support deception.

Close, consistent technical study is required for emerging Russian C2D system's potential utility and application. There are a number of actual REB systems that are continually updated and can be placed in specific functional categories if properly analyzed. They may require specific counters in case the West, at present, has not considered their extensive and perhaps unique applications. Thus, there is much for Western analysts to consider when examining Russian REB concepts and capabilities and perhaps use some issues to further develop Western EW concepts and capabilities.

The article discusses Western concerns about Russian REB and the latter's focus on Western weaknesses and capabilities. It covers Lastochkin's and other's claims that REB is the key to controlling future operations, and closes by highlighting prominent military discussions of REB as a concept from 2015 to 2018 by both active and retired officers.

Table of Contents

Introduction

Military and political leaders in nations around the globe are always on the lookout for ways to solve their national security dilemmas. Once these issues are theoretically and technically resolved, leaders feel more secure in their ability to attend to current and future threats. Military leaders in turn feel empowered to impose their will, if necessary, on potential adversaries with these advanced concepts and capabilities.

Such capabilities, according to one senior Russian officer, are close to being turned into reality in its Armed Forces. Major General Yuriy Lastochkin, who is in charge of the Defense Ministry's radio-electronic warfare (REB) force,[1] stated in 2018 that REB's men and equipment will permit Russia "to decide the fate of all military operations" in the near future.[2] This is quite a surprising statement when contrasted against President Vladimir Putin's focus on advanced weaponry (hypersonic and strategic missiles, nuclear torpedoes, equipment blinding lasers, etc.), which made no mention of REB capabilities. Perhaps this is just a specific military branch chief's pride in his force, or a military perspective versus a political one.

Or, perhaps REB represents the asymmetric answer that both General Staff Chief Valery Gerasimov and Putin have called for to offset Western high-technology superiority in other areas. A 2019 article in the Russian journal *Military Thought* noted the nation's military-technological asymmetric response must deter an adversary from launching a large-scale war. Russia can do so, the article stated, by creating the threat of using asymmetric systems such as electronic warfare countermeasures.[3] Another article stated that REB assets "are one of the main asymmetric means of waging new-generation wars."[4] REB is asymmetric in that it is not so much a force on force concept but rather a way to unravel a force simply through an indirect method, attacking frequencies; and REB uses this indirect method to achieve another asymmetric effect, the disorganization of an opponent's command and control (C2) capability. This is a powerful way to confront either the West's anti-access, area denial (A2AD) concept in particular or the contested environment in general.

The disorganization topic is quite prominent in Russian military literature. It has been the centerpiece of several recent articles in military journals and is underscored in interviews with leading REB experts year after year. Thus, it is not just A2AD but the "C2D" (command and control disorganization) concept that should concern those watching Russian theoretical developments, especially in light of Russia's perceived view of the US as having attained only a limited electronic warfare capability. REB frequencies that disrupt systems (UAVs, EW equipment, radars, etc.) and disorganize C2 cause chaos in planning, inhibit the coordination of efforts, and lead to the defeat of an opponent. The concept is now enhanced even further with a military decision to create a "disorganization plan" in each REB brigade to better confront adversaries. Perhaps the disorganization issue was practiced most recently and vividly during Vostok-2018, when a massive REB strike was practiced for the first time on such a large scale, resulting in the jamming of the adversary on land, on sea, and in the air.[5] That is, the plan was to create total disorganization. Various Russian officers reference the concept nearly 30 times in the sections that follow these introductory remarks.

But returning to Lastochkin's contention that REB will decide all military operations, there are many capabilities that support his claim. For example, Russia's Divnomorye mobile complex is simultaneously a reconnaissance station and a jamming device. It purportedly can conduct targeting interference on numerous US systems, such as helicopters, unmanned aerial vehicles (UAVs), long-range radars, E-3 AWACS, the E-2 Hawkeye, and the E-8 JSTARS, as well as spy satellites.[6] If true, then just this one system

could affect the fate of several aspects of military operations. The same report noted that Russia will be creating a REB battalion for every combined-arms army. Previously such units were only at the disposal of military districts.[7] Today Russia has more than 30 different REB systems in the ground forces alone to attack UAVs, radars, GPS frequencies, cellular networks, and other command and control or communications devices. One system to combat UAVs even utilizes electronic rifles.

Lastochkin believes that REB can create an electronic dome over the battlefield, shut down adversary systems at will, and debilitate the eyes and ears of an adversary. Regarding the latter, for example, along the strategic Northern Sea Route the Murmansk-BN system is designed to interfere with communication systems, ship navigation and control systems, and submarines and aircraft that illegally cross borders. If realized, he asserts a system like this would suppress any intruders[8] and totally control access to the region by making them blind and deaf.

A recent Russian exercise worked to create a vacuum or safe zone (electronic dome) over troops to protect them against drones, airborne radars, radio-controlled explosive device, and cruise missiles. This was accomplished through the use of three systems working together:

1. a Borisoglebsk signals intelligence gathering capability;
2. a Krasukha system's ability to suppress aircraft radar emissions and a drone's radio control channels; and
3. a Zhitel system's capability to jam satellite communications, navigational equipment, and cellular communications to a radius of 30 km.[9]

Attempts to Strike Fear in NATO and the US

Numerous Russian articles claim that their military's REB systems are far superior to Western ones. Western EW weaknesses, they note, are many and have been exposed.

There may be two purposes for these and other such reports. First, it could be a bluff -- a way to deter NATO and the US by implying that Russia has superior capabilities, even though they don't. Deterrence works in that way, using fear. Or, it could be that Russia has some of these capabilities (but not all of them) and is willing to demonstrate those they have. Russia is demonstrating its capabilities, as Norwegian and Finnish officials state, and such abilities can act as a deterrent through the introduction of doubt about just how secure other nations' systems really are. Russian analysts are not shy in pointing out their own competency and their consideration of Western EW limitations.

Regarding Western weaknesses, Russian officials write that practically every US weapon is hooked to satellite communications, GPS navigation, and the mobile Internet. REB operators claim to be able to shut these channels down with ease. Recent DARPA contracts, Russian analysis notes, appear to focus on weak systems to upgrade. DARPA is directing companies to design new systems able to function against electronic interference.

Another Western concern is that Russia is not limited to just jamming NATO systems but can also intercept and manipulate US military targeting data. One US analyst, according to the same Russian publication, stated "If the enemy can get into command and control computers to provide wrong data, you could potentially call in airstrikes against your own positions. If troops can no longer communicate, close air support becomes more time-consuming or impossible."[10]

A second Russian report stated that US concern about Russian REB superiority is buttressed by Russia's successful intrusions into the electronic systems of other nations. The Norwegian Defense Ministry blamed Russia for GPS malfunctions during the 2018 NATO Trident Juncture Exercise. Finnish Prime Minister Juha Sipila stated that jamming from the Kola Peninsula had knocked out some of his nation's navigation systems during that same event.

Israel implied that the Krasukha-4 REB complex was to blame for the recent inadequate performance of its Iron Dome air defense system. With an operating range of 300 kilometers, the Krasukha system could reach Israel if deployed in Syria. Zhitel, Divnomorye, or Borisoglebsk-2 systems may also be at fault, according to Israeli experts cited in the Russian report. None of these nations claim to have potential counters to these Russian systems.[11]

Former US Army EW chief Laurie Buckhout was cited in the report as having stated that Russian REB capabilities surpass those of the US by orders of magnitude, the reason being that the US has not fought against capable functioning radio communications for decades and thus has put less focus on these systems. Whether Buckhout made the comment about "orders of magnitude" is uncertain, but in other publications she expressed concern over the growing capabilities of Russian systems.

The US Army's Asymmetric Warfare Group was less pessimistic, noting a year and a half ago that "For an anti-access, area-denial, or A2AD bubble to protect Russian brigades in a major ground operation, Russian forces would need larger numbers of EW and air defense platforms than they have. Nearly all such platforms are in Kaliningrad, Ukraine, and Syria."[12] Today things are different for Russia's military, as it reportedly has a REB brigade in each military district and there are companies in tank brigades and divisions.[13]

Retired US Lt. Gen. Ben Hodges, former commander of the US Army Europe, did not say Russia's capability was greater than NATO's but noted their EW capability is:

> Something we never had to worry with in Afghanistan and Iraq. The Ukrainians live in this environment. So, you cannot speak on a radio or any device that's not secure because it's going to be jammed or intercepted or worse, it's going to be found and then it's going to be hit.[14]

Finally, Russia states that their competency has advanced to the testing of electromagnetic weapons, which can be regarded as the further development of electronic warfare devices. One such weapon is the Alabuga. These jammers explode at a height of 200-300 meters and shut down electronic equipment within a radius of 3.5 kilometers. The system takes out electronic components in the affected areas out of commission.[15] Another is the Afghanit system, a microwave weapon now fitted on military vehicles. There appear to be specific projects for the creation of electromagnetic weapons, which include projectiles, bombs, and missiles that carry magnetic explosion generators to burn adversary electronics or the homing heads of missiles.

A Russian Defense Ministry Website offered an opinion on the performance of such weapons:

> Ultra-high-frequency weapons (microwave weapons) are a type of electromagnetic weapons whose harmful effects come from super-powerful electromagnetic radiation in the microwave range (0.3-300 GHz). They are intended to disable radio-electronic and optical elements of equipment and weapons (including space objects), suppress air defense and antimissile defense systems, disorganize control, protect against high-precision weapons, and so on.[16]

Another report stated that electromagnetic guns are continuously being tested in laboratories and firing ranges in Russia. They will be able to disable the warheads of self-guided missiles, and could be installed on UAVs.[17]

Russian reporting on REB systems is sometimes overstated, especially regarding their capabilities (see, for example, the discussion of the Zaslon-REB in the Appendix at the end of this article). However, Russia does possess impressive REB capabilities and is clearly willing to discuss and demonstrate them.

Russia's Chief of Electronic Warfare

One of the chief sources of information about Russian REB is its commander, Lastochkin, who has offered interviews and written articles since 2014. His interviews/articles are summarized below. Added to the discussion are three 2019 separate REB discussions. One is a short interview with another REB major general and the other two REB-associated articles were found in the Russian ground force journal *Armeyskiy Sbornik (Army Journal).*

In 2014 Lastochkin, a colonel in charge of REB at the time, noted that radio-electronic systems provide the technical foundation for most of the state-of-the-art armaments and military equipment. He viewed the employment of REB methods against high-tech items as an asymmetric measure designed to nullify an adversary's ability to wage armed combat. It is desirable to engage an adversary's assets on his own territory and to use "the emergence of assets for the functional kill of an adversary's electronic assets…and the employment of special assets to disrupt the operations of computerized command and control systems built on the network principle."[18]

Among them are:

- Selecting C2 and intelligence-gathering systems as priority targets:
- Developing new ways to disrupt radio wave propagation;
- Creating technologies to reduce armament signatures;
- And employing assets creating a complex REB environment for an adversary's technical reconnaissance and intelligence-gathering facilities.[19]

In 2015 Lastochkin wrote on REB's future in the journal *Military Thought*, concentrating on offense, which included jamming opponents and then attacking them with REB. The latter becomes an asymmetric response to level the other side's advantages, such as an adversary's high-tech weaponry.[20] An adversary's REB assets can be suppressed to the full depth of his operational order of battle and effects can be similar to those possessed by high-precision munitions, he noted. REB can be used alone or with fire assets and special operations forces to gain information superiority; and it can perform information warfare missions to protect against technical reconnaissance assets. Lastochkin correctly predicted that REB's capabilities will allow it to play a larger role in conflict, raising its status.[21]

In 2016 he noted that a special REB troop range would be created by 2018. The range will offer units compressed time periods to execute missions and will include specific operational-tactical situations and the opportunity to organize coordination on a planned virtual battlefield. The Magniy-REB simulator training complex is being supplied to help carry out this training.[22]

In 2017 Lastochkin noted a new arena of confrontation had emerged, the information and telecommunications environment. REB missions had expanded their effectiveness, such that their

employment "is comparable to the effective engagement of the target with precision weapons."[23] REB forces are designed to engage adversary facilities and offer the integrated control of countermeasures against an adversary's technical means thereby protecting friendly forces. REB forces are:

- Building electromagnetic radiation weapons;
- Developing software that can disrupt the accessibility, integrity, and confidentiality of adversary information;
- Applying the means to mimic false electro-magnetic environment and deceive adversary systems;
- And improving decision-making algorithms through a single C2 loop.[24]

Lastochkin singled out the Zaslon-REB system as a guaranteed capability to block channels where information might be leaked by establishing an electronic dome over the Defense Ministry's facilities and installations. He stated that REB is the "sole effective method of combatting miniature UAVs."[25] Training time has doubled for REB operations, and the volume of missions in a strategic section "will increase by a factor of 100-150 percent" and will form the basis for an effective air-ground REB system.[26]

The military newspaper *Krasnaya Zvezda* also interviewed Lastochkin in 2017. He said new REB systems can neutralize a probable adversary's electronic hardware countermeasure systems; and introducing disinformation into an adversary's C2 system can deceive him regarding Russian troops actual concept of operations and the location of its military facilities. REB missions included ensuring the electromagnetic compatibility of electronic systems, the international legal protection of military electronic systems, and planning for the use of radio frequencies. Russia also plans to complete the integration of electronic warfare information resources into the Armed Forces Single Information Space, which will provide command authorities the ability to use all the information about the operational and electronic situation for the organization of REB.[27]

Lastochkin's most important REB article may have been written in 2017 in conjunction with three other analysts for *Military Thought*. They discussed how REB had become an important method of implementing operational art. The latter is in a continuous state of development, depending on "the emerging military and political situation, the quality of weapons and equipment standards of one's own Armed Forces and foreign armies, as well as changes in the views on conducting combat actions."[28] Further, REB forces are integrated into reconnaissance-fire-and-strike systems, which provide real-time responses to target identifications. This makes disorganizing adversary C2 more of a priority, and may increase REB's prominence and influence within the Russian military two or three-fold.[29]

REB methods were singled out for discussion. The analysts recommended "a tree of combat employment methods at the head of which there should be methods of disorganizing adversary C2."[30] These can be various fragmentation methods. Fundamental disorganization methods include an information blockade of C2 bodies and information blocking of complex electronic equipment.

Finally, there are physical methods of disorganizing, such as destruction, distortion, and misinformation. These would include destroying circuitry with electromagnetic radiation or using special programs to impact software and databases.[31] With the REB force under consideration to become the fifth arm of Russia's ground forces (after motorized rifle formations, tanks, artillery, and air defense assets), operational art basics are still needed. They must, the authors note, be both original and unorthodox.[32]

Lastochkin solicited help in compiling a thematic anthology titled "Electronic Warfare in the Russian Federation Armed Forces," to include organizations and enterprises developing EW systems, problem issues, and tasks facing military experts and developers of modern EW systems. Information about current and future projects would also be provided. The website (www.reb.informost.ru), should be up-and-running.[33]

Lastochkin took the bravado to new heights in a 2018 REB Day interview. The following three quotes summarize all his major points:

> I will say more: qualitative changes in the development of **electronic warfare** men and equipment will permit them to **decide the fate of all military operations** already in the near future. The matter is for the practical realization of the potentially high prospects for contemporary electronic warfare. The **disorganization of enemy troop and weapons command and control** and the reduction of the effectiveness of the conduct of reconnaissance and weapons employment by them **is the primary goal of the conduct of electronic warfare**. With respect to the spatial scale, we are capable of accomplishing missions on a global scale in individual physical fields, in other words, to selectively carry out jamming against facilities, which are located practically at any location of the world and outer space. Our **equipment's capabilities permit us to create, as you say, a 'dome' not only over a missile complex** but also to provide full-fledged protection from air and space reconnaissance, for example, of a major command post or the country's other important facilities.[34]

The focus on disorganization was underscored in a report three days later about US airstrikes on Syria due to the latter's use of chemical weapons. Lastochkin stated, "It is impossible to achieve superiority over an enemy, which is achieved through the disorganization of his information management and telecommunication systems, without state-of-the-art electronic warfare systems."[35]

Lastochkin's 2019 annual article noted that REB is the main form of operational (combat) support and that it aims to disrupt adversary information systems through suppression of transmission channels. He stressed that fitting REB systems to missiles, combat aircraft, helicopters, warships, and armor is being accomplished, to protect them against intelligence gathering and precision weapons. REB assists are used to reduce the detectability of many types of equipment, to include the Su-57 fighter, Armata, Bumerang, Kurganets, and Tayfun armored vehicles, and surface warships such as Project 20380 and Project 22350 corvettes.[36]

Another important interview was that of Major General Sergey Klindukhov, Chief of the Eastern Military District REB Headquarters. He stated that an adversary's destruction is accomplished via the employment of both traditional strike weapons and electronic reconnaissance and suppression complexes. He made one very interesting comment about combat operations, which provided an indication of how Klindukhov felt future wars would be conducted:

> Contemporary armed conflicts are characterized by surprise and short duration and a dramatic change of the operational situation. And the primary factor, which influence success in operations, is the seizure of the initiative and superiority in the information environment through rapid decision-making and immediate reaction to threats…[37]

Klindukhov stated that electronic facilities are now mobile and include remote control or programmed command and control methods. He mentioned that the Silok and Pole-21 jamming complexes can block an adversary's UAV remote control and suppress its transmission of photo and video context and target coordinate data. REB mobile teams have also been created, one with a Borisoglebsk-2 complex, to detect radio sources and jam an adversary's C2 channels.[38]

Armeyskiy Sbornik (Army Journal) carried a few recent articles on how to use REB to hamper an enemy force. One article devoted to missile troops and artillery noted that the problems for REB to solve involve increasing the effectiveness of disorganizing enemy command and control, fire control, reconnaissance, and REB. The Rtut-BM and Infauna systems were highlighted for their importance. The article concluded by noting "in future wars the outcome of combat operations also will be determined to no small degree by the potential of REB."[39]

A second article noted that the consequences of even an insignificant failure in the C2 sphere can rapidly and irreversibly affect the course of an operation (engagement) as a whole. This demands C2 superiority, as it can define the operational efficiency and quality of day-to-day (local) decisions. Future operations will requires C2 information support close to real time and with reference to the current situation.[40]

Military Thought Articles, 2015-2019

In 2015 three authors noted that REB is conducted to disorganize adversary troop and weapons control and thereby achieve superiority over an opponent.[41] REB tactics depend on the forms in which they are employed, and the methods used to fulfill combat tasks. Russian commanders closely study an adversary's electronic systems and assets to inform about adversary strengths and weaknesses. Such criteria provide the input that allows for a commander's creativity on the battlefield.[42]

REB abilities include jamming communications, radars, and radio navigation systems of an opponent, and the ability to then hit them with fire from other assets.[43] REB goals are:

- Accomplished through the massive and joint employment of forces at selected stages of an operation;
- Through the extension of the zone of combat to an adversary's full depth and the use of REB maneuver units and systems of electronic strikes;
- And through close cooperation with REB and other tactical units.[44]

In 2016, one article noted that REB is a main asymmetric way of waging war. The author added that REB's main capabilities must be concealed from probable enemies to the maximum extent and be a surprise when the tactics employing them are unleashed. REB equipment should rely on domestic components and there should be an active development of millimeter and terahertz bands of working frequencies.[45] The goal is to create a difficult electronic environment for an adversary's troops.

Russia has also established some REB institutes (Electronic Warfare Scientific Research and Test Institute as part of the Zhukovskiy and Gagarin Air Academy; the EW Troops Military-Scientific Committee; and two science companies for REB), among others.[46]

Another 2016 article included a discussion of REB methods. It clearly stated, "target orientation lies in disorganizing the adversary's information support for combat actions and the guided weapons used by him."[47] Tasks include the following:

- Disorganizing the adversary's information support when he directly controls combat activities during an operation;
- Disorganizing the adversary's information support when he employs guided weapons;
- And disorganizing the adversary's information support electronic warfare forces (counter EW).[48]

Jamming, naturally, is the main method to disorganize an opponent, of which node jamming is a specialized aspect.[49] Delaying timely information support to decision-makers, misguiding them with false information, constructing information blockades, warping databases, and destruction are other methods.[50]

LTC O. G. Nikitin, a Russian military EW specialist writing in *Military Thought*, predicted the principal content of future operations will be the struggle against information infrastructures. A prominent role in disorganizing these structures belongs to REB forces, he wrote in 2017. These no longer appear to be a support force but an independent force with its own missions, methods, and forms of combat employment.[51] He noted that a decision-making support system (DMSS), a higher form of information technology, will be designed to disorganize an adversary's executive elements. He stated that a DMSS of a REB force's command and control organ would be understood as

> A hardware and software complex that makes it possible for the appropriate officials at all stages of the organization and direct employment of REB forces (troops) and means to resolve both structured and non-structured tasks with respect to forming rational decision variants on the combat employment of various forces and means enlisted to accomplish the task of disorganizing enemy command and control of troops and weapons.[52]

Software, linguistic, information, mathematical, and technological support are all elements of the DMSS concept. The most critical adversary C2 processes and organs taking part in the DMSS must be identified. It is first necessary to develop an appropriate disorganization plan, a model of the adversary's C2 system, and the adversary's critical information areas.[53]

This requires identifying the operational, information, and radio-electronic situation, which assists in the identification of targets and helps with allocating the resources of other branches to disorganize enemy C2. The assessment of an opponent's operational situation involves examining his correlation of forces, forecasted changes, and an opponent's most important C2 organs. The information situation involves identifying the level of informatization of C2 organs and critically important targets, with the latter understood to be that which carries out the receiving, processing, sorting, and transmitting of information. The radio-electronic situation is a component of the operational and information situations, assessing numbers, characteristics, conditions, capabilities, methods, and sequence of use. According to Russian writings, it is important to select C2 processes that disorganize and sharply reduce an opponent's combat operational effectiveness at both specific stages of an operation or for the operation as a whole.[54]

C2 processes identified as targets are known as fragmentation targets. Nikitin stated it is possible for each set of fragmentation subjects to propose specific methods of disorganization (types of fragmentation) and the type of effects utilized depend on the makeup of friendly forces. The ultimate aim is to select the appropriate forms and methods of use. The latter could include blocking C2 organs or information support elements.[55] The REB chief must be presented with one or several variants of a plan to distribute forces and means against targets identified in the operational, information, and radio-electronic situations. The plan is coordinated with fire destruction resources as well.[56] Of interest is that Nikitin used the term disorganization 21 times, making it truly a goal of Russian REB formations in his opinion.

Another 2017 article discussed the development of weapon strategies, defined as traditional (the progressive development of existing weapons); innovative (new-generation weaponry is anticipated via the use of artificial intelligence technologies, etc.); and breakthrough (creation of fundamentally new and nontraditional models).[57] The actual goal of REB development is integrated use of all three strategies, where the proportions between principal supporting strategies must be justified and an optimum balanced correlation of strategies implemented. Traditional strategies may predominate in a period of threat, innovative strategies when the threat is unclear, and breakthrough strategies when there are no visible threats.[58] Research criteria included understanding the forms and methods of employing REB forces and methods for disorganizing enemy command and control systems.[59]

A 2018 article addressed ways to attain command and control superiority in ground operations. C2 superiority was deemed an operational goal that must include information and intellectual superiority for decision-makers in addition to military and technological superiority. Primary targets for disorganizing an adversary are the latter's control bodies and troop and weapons control systems. The authors noted it is important to isolate an adversary's C2 structure from information critical to determining the course and outcome of combat actions. This is primarily accomplished by impacting electronic assets that service C2 bodies. Disorganizing information support systems is most important.[60]

Recommendations

For Western analysts, recommendations from this analysis include:

The West needs to stop mirror imaging. There is one Russian refutation after another that they do not spend time conducting hybrid warfare. Instead, it's the West that uses the concept against Russia. Instead, Russia is focused on asymmetric actions and ways to disorganize an opponent, including through the use of EW. Understanding adversarial capabilities and methods that Western practitioners have not considered to date will make their own concepts stronger. This will require close study of Russian REB tactics and techniques to scope out which are new and potentially useful to Western practitioners.

The West must follow and better understand these disorganization concepts as Russia further refines them. While the West worries about Russian A2AD concepts, it is more likely that Russia is putting together a program that will cause chaos in Western control systems through the disorganization of adversary command and control. The Russians are now expanding the use of REB as an independent branch, experimenting with REB maneuver units, and focusing on developing a disorganization plan for use in each REB brigade.

Start watching what theories are blending into real actions during exercises, which will provide better input and expectations from Russian intentions. Russia appears to be experimenting with C2D in live engagements, such as the attempts to disrupt NATO exercises like Trident Juncture. It is training with C2D via systems like Murmansk-BN to protect its Northern Sea Route and access to vital resources there.

Western specialists need to become more aware of how REB could be integrated with deception techniques. This requires an understanding of Russian maskirovka, spoofing, and reflexive control techniques and the equipment (inflatable equipment, fake frequency sources, etc.) developed to support deception.

Close, consistent technical study is required for emerging Russian C2D system's potential utility and application. There are a number of actual REB systems that are continually updated and can be placed in specific functional categories if properly analyzed. They may require specific counters in case the West, at present, has not considered their extensive and perhaps unique applications. Thus, there is much for Western analysts to consider when examining Russian REB concepts and capabilities and perhaps use some issues to further develop Western EW concepts and capabilities.

Conclusions

Lastochkin believes that REB operations will decide the fate of all military operations. His bravado indicates he finds "asymmetric and A2AD gold" applying REB capabilities against what Russia considers a major Western weakness -- the latter's numerous links to space assets. There is certainly ample evidence to suggest that a significant REB capability is under development. There are numerous REB systems in Russia (see Appendix below) that handle various missions. They can create distorted navigational fields, suppress radio-controlled mines, obtain bearings of electronic wave emission sources, and create interference

against adversary communication systems. Jamming opponents and conducting electronic strikes against them enable the disorganization of an adversary's force.[61] In some exercises, decoy lines of communication are created in an adversary's networks and command posts and artillery positions are covered with an electronic umbrella to keep them safe from a precision missile strike.[62]

Of note was the consideration that REB no longer appears to be a support force but an independent force with its own missions, methods, and forms of combat employment. Another important point was the use of REB capabilities to deceive opponents into carrying out instructions that had been interfered with or manipulated by Russian forces. Of course, the consistent use of the term's "disorganization," "disorganize," and "disorganizing" used throughout the discussion indicated that this is a major method for attaining superiority and is a focal point for REB operators and planners. For this reason, the C2D concept was suggested as an adjunct to the more commonly used A2AD reference. REB maneuver units were another interesting development.

Systems are often integrated. For example, in the Eastern Military District on REB Day in 2019, state-of-the-art jamming stations, namely the Leer-3, Zhitel, and Rtut-BM were deployed against an aggressor communications center.[63] The same day a Leer-3 UAV, a Zhitel automated jamming station, a Borisoglebsk-1 system, and a Lava-RP cellular communications jamming system worked together in another exercise.[64]

On REB Day 2019, *TASS* singled out electronic intelligence collection and the destruction of adversary command and control systems as the most important REB missions. This is how you disorganize an opponent and develop chaos in his force. The article noted that REB units are proliferating throughout the Armed Forces, adding:

> In the ground troops, separate REB brigades were formed in all four of the military districts. There are companies in tank brigades and divisions as well as within the ranks of the Airborne Troops. In addition, there is also a similar subunit in the Arctic motorized-rifle brigade. In the Navy, ground REB forces are combined in separate centers in all four fleets. In the Aerospace Forces, there are separate REB battalions in the order of battle of the Air and Air Defense Armies.[65]

Thus, there appears to be a serious focus in Russia on REB capabilities. It is rising in importance as an asymmetric way to counter A2AD capabilities and a way to deceive or, most important of all, disorganize an opponent. REB is asymmetric in that it is not so much a force on force move as it is a way to unravel an opposing force through indirect methods, attacking frequencies. REB's ability to disorganize A2AD force planning is seldom considered in the West, where the focus is primarily on countering missiles and aircraft. Seizing the initiative in REB allows Russian forces to quickly implement decisions while seriously hampering an opponent's decision-making abilities, especially when deceptive measures are employed.

Appendix A
Russian Ground, Air, and Naval REB Equipment

[REB systems for which no information could be found in the last three years include the ground system Parodist; and the Navy systems TK-28, MP-411, KT-308, Prosvet-M, MDU-2, and Ugolok].

A:1 REB Equipment

A:1.1 Ground Forces:

Spektr—On REB day 2019 the Southern Military District stated that the mobile technical viewing and monitoring complex Spektr was employed by electronic warfare subunits. While this may not be a piece of REB equipment, it is one of several reconnaissance assets used by REB operators. It is designed to track designated territories where dangerous objects could appear via air optical-electronic, ground optical-electronic, and radio and radio-technical monitoring. REB specialists used the complex to conduct surveillance and the detection of targets, information that was then passed to command authorities.[66]
Avotobaza—This system combats UAVs by disrupting communications. It has been described as a ground radar jammer, an electronic intelligence system, and a radio-technical reconnaissance system.[67]
Brisoglebsk-2—The systems jamming stations electronically suppresses an aggressor's command and control system's components.[68] The system collects and analyzes reconnaissance information and generates radio interference, which limits an adversary's ability to use precision guided weapons and to conduct reconnaissance.[69] It can suppress the signals operating a UAV within a radius of 30 kilometers.[70] During one exercise using the Borisoglebsk-2, servicemen created decoy radio communication lines inside a hypothetical enemy radio network to provide cover for friendly infrastructure.[71]
Bylina—This system independently selects and identifies targets (radio stations, communication systems, radars, long-range radar detection aircraft, satellites, and other facilities) within seconds. It decides how to effectively suppress them and selects the jamming stations to do so. It operates in the short-wave band.[72] It automatically interfaces with battalion and company command posts and individual REB stations. It specifies the sequence of actions after identifying a situation and conducts operations that do not affect friendly REB stations. The system uses artificial intelligence algorithms for the conduct of automated decision-making.[73]
Dzyudoist—The system can jam the signals of radio-controlled high-explosive rounds. The term means "Judo Fighter." It is an automated system that can also jam cellular communications. The system uses radio interference to disrupt a range of frequencies and to disable a navigational system, such as that of a drone, from more than 50 kilometers away and prevent them from approaching the forward edge of their troops.[74]
Filin—This optical jammer is designed to dazzle enemy optical sensors, both visual and electrical. For those soldiers or sailors (the system is now being placed on ships) using sights for firearms or other weapons, it modulates bright light beams, where low-frequency oscillation causes agitation of the optical nerves, producing a temporary and reversible disruption to one's sight. It was reported that one in five soldiers experienced hallucinations, while about half felt disoriented and dizzy/nauseo2019.us. The system can affect laser rangefinders in the infra-red range, night-vision devices, and guidance systems for anti-tank guided missiles up to five kilometers. The export version is reportedly the Grach.[75] The effective range is 500-700 meters in a sector 10-15 degrees wide. It is called a nonlethal weapon.[76]
Grach—This system is, as implied in the Filin discussion above, a similar system. It is simpler and lighter and can be installed on second-tier surface ships and on armored and specialized vehicles for security bodies. The systems liquid cooling allows it to be used in various climatic conditions. It can jam television and thermal devices, or electro-optical equipment that is used for detecting targets. It can be used by the Navy or Ground Forces.[77]

Infauna—The system can suppress operations of an adversary's radio-electronic communications means and various types of UAV navigation systems operating at a distance of up to 100 kilometers in mountainous terrain.[78] It can jam radio communication lines for remote-controlled charges and mines.[79] A recent report noted that, using an aerosol jamming system installed on an Infauna complex, it was possible to hide a convoy and simultaneously jam radio communication lines that controlled an adversary's remote-controlled mines along the convoys path.[80]

Leer-2—This system conducts electronic intelligence reconnaissance of radio radiation and jams electronic equipment. It can simulate operations of various electronic systems and conduct an assessment of the electromagnetic situation.[81]

Leer-3—This complex has three Orlan-10 UAVs and is known as a smart UAV, since it is fitted with the capability to jam 3G and 4G mobile communications, conduct reconnaissance, and transmit data to artillery crews. It can send out mass SMS messages to cell phones[82] and can disable remotely controlled explosive devises of illegal armed formations.[83] It can be classified as a virtual cellular station and it can send out audio messages and small video clips. The Orlan-10s have jammers on them as well as disposable jammers that can drop to the ground. The Leer-3 is designed to suppress the Global System for Mobile Communications (GSMC) networks.[84]

Lesochek—The system's jamming stations prevented radio-controlled IEDs, that were camouflaged along a movement route, from detonating.[85] A mobile closed radio zone, organized by installing small scale Lesochek jamming stations on combat vehicles, was also developed based on experience gained in modern military conflicts.[86] A report noted that the system can disable enemy satellite reconnaissance systems and radio traffic as well.[87] Another report stated that the Lesochek's frequency band is three times wider than its predecessors and that it can be carried on vehicles, in a backpack, or in a briefcase.[88]

Less—The system has integrated equipment monitoring command and control posts and portable radio monitoring complexes that would be used during the training assemblies.[89]

Leyer-3—This system suppresses enemy electronic resources and makes it possible to perform such tasks at a distance of more than 100 kilometers from the subunits' place of deployment for a period of 10 hours.[90] The system can block equipment operating in the GSM-900 and GSM-1800 bands. It was noted that "there is the capability of shutting down the bands of all cellular networks of a simulated enemy within a radius of six kilometers with jamming from a special UAV."[91]

Lorandit-AD—This airdroppable system is supplied to the Airborne Forces. It uses direction-finding to suppress illegal armed formations and sources of interference.

Krasukha-2.0—The system is designed to search for and jam any ground-based and airborne radars. It blinds and deafens aircraft at a distance of 300 kilometers and intercepts command and control channels of unmanned aerial vehicles and cruise missiles.[92]

Krasukha-S4—The system combats aviation radars, communications, and data transfer systems. It can jam the signal of all current radar stations. The system's estimated range is 150-300 kilometers.[93] The system protects convoys from UAVs.[94] One article noted that it can cover several hundred kilometers of territory with an umbrella that is impervious to electromagnetic waves. It can stun long-range radar aircraft or space satellites used to guide missiles to targets. It can burn out electronic systems of aircraft, missiles, and satellites in low orbit. Finally, the system can create the appearance of targets yet withhold identifying information, making a determination of friend or foe most difficult.[95] Russia might supply Syria with state-of-the-art Krasukha-S4 electronic warfare (EW) systems, but it's going to be adjusted for this region both in terms of software and intellectually. It will have its own electronic memory and will be fully integrated with air defense systems, anti-aircraft missile systems, radio-engineering systems, and fighter aircraft so that it can operate as part of a combined control system.[96]

Moskva-1—The complex includes an intelligence collection module and a command-and-control post for jamming subunits (stations). The complex can conduct radio and radio-technical intelligence collection at ranges up to 400 kilometers; classify

all radio emitters according to threat level; provide air surveillance support; support target allocation and imaging of all data; and support reverse monitoring of the effectiveness of the subunits separate EW asset operations, which it commands.[97]

Murmansk-BN—It is used to conduct electronic reconnaissance for communications and radar site detection of ground and airborne reconnaissance, and to conduct concentrated electronic strikes at aggressor command and control and communication systems.[98] The system was deployed on Kamchatka such that, along with the Krasukha and Divnomorye systems, the entire Northern Sea Route will be covered by REB forces. The systems can interfere with communication systems, navigation and control systems of ships, and submarines and aircraft that illegally cross borders. This ensures that Russian can suppress any intruders.[99] The Murmansk-BN is present in the Kaliningrad Region as well. It can jam military communication networks at ranges up to 5,000 kilometers and in some conditions up to 8,000 kilometers. The system is a short-wave shore-based REB system that can gather electronic intelligence information and can intercept and jam signals in all shortwave bands;[100] and it can operate at an operational-tactical and operational-strategic level. The system entered service with the 841st Separate EW Center of the Baltic Fleet at the end of 2018. It may include several EW battalions and companies to carry out combat missions.[101] The technology allows for "disorganizing any system of shortwave communication."[102]

Orlan-10 UAVs—This system, and probably other UAVs, not only can conduct reconnaissance and generate targeting data for fire resources, but also can block GSM-standard cellular communications and distort the navigational field for GPS systems.[103]

Palatin—This is an operational-tactical level REB system that can suppress existing and future radio communication systems of an adversary; conduct electronic reconnaissance; blind an adversary with short-wave and ultra-short-wave frequencies; deprive an aggressor of his cellular and trunked communications; and integrate various friendly REB and electronic reconnaissance systems into a single working network.[104]

Pishchal—This is a counter-drone gun whose operating range exceeds two kilometers.[105]

Pole-21—The system has suppression/jamming modules designed to counter drones and reduce the effectiveness of cruise missiles. It is being provided to the Central Military District. It will cover vital military and civilian infrastructure and provide security from the use of high-precision weapons. It can suppress signals going through various satellite channels, to include GPS, Galileo, and Beidou.[106] Further, the system's equipment allows for the installation of up to 100 radio jamming posts in a shielded zone and each has 1-3 modules with a suppression range outside the zone of up to 150 square kilometers. The remote-controlled maintenance-free modules can be installed on cellular network towers up to 60 meters in height and operate in various temperatures.

REX-1—This system is an electronic rifle that can protect forces from UAVs. It suppresses drone signals and has an operating range of 500 meters, with the signal propagating in a 30-degree sector. The rifle can block GPS global positioning systems signals in a radius of two kilometers. A drone's optical-electronic devices are suppressed as well, both the reconnaissance and the missiles seeker head.[107]

Rtut-BM—This electronic warfare complex counters enemy munitions equipped with radio-controlled detonators.[108] The system is designed "to protect manpower and equipment, provide cover for troops concentration areas, separate stationary and mobile facilities, and is capable of neutralizing shells, fitted with proximity fuses, on a territory measuring up to 50 hectares."[109] The system creates a "dome" over a protected site, causing shells to detonate at a safe distance or deactivate.[110] It can jam frequencies used by an adversary for radio communications.[111]

Samarkand—This system jams high-precision weapons such as the US Tomahawk.[112] There are 13 Samarkand-U, Samarkand-SU-PRD-K2, and Samarkand PU-PRD-D complexes on Russian territory, designed to generate interference and disrupt an adversary's communications.[113]

Sapsan—This system has an operating radius of 100 kilometers. Its search capabilities include radar, the visible and infrared optical ranges, and electronic reconnaissance. It conducts a directed

flow of electromagnetic jamming that halts an attack from a swarm of drones from a single axis.[114]

Serp—This system is mounted on an air defense complex (BUK) chassis and can handle swarms of small drones. It is a microwave gun that burns electronics. An active phased array antenna detects the drones at a range of 20 kilometers. The system can also target precision-guided munition seeker heads.[115] The system blocks and suppresses the control and navigation channels of a UAV; and it can pinpoint who and from where the UAV is controlled up to 3 kilometers from the object. The directional antenna conducting this work has the name "Cheremukha (cherry)."[116]

Shipovnik-Aero—This system has a 10-kilometer range, and it can take over a UAV's command and control if the drone's model is in its memory. It can determine the coordinates of the location from which the command and control is being conducted with an accuracy of 1 meter for transmission to an artillery battery.[117]

Silok—The system jams UAVs of various types at a range of more than four kilometers and across a wide range of frequencies.[118] The system detects UAVs automatically, independently determines their coordinates, and jams the control, telemetry, and communications channels of the equipment.[119] One report noted that Silok and Zhitel systems were used in Syria and they applied this experience during Vostok-2018.[120]

Solyaris-N—The system is said to be a brand-new smart system for protecting a site against drone intrusions. It can reportedly protect an area of up to 80 square kilometers against automated means of aerial reconnaissance and attack. The complex works automatically, without an operator. It detects an airborne object, analyses the trajectory and also the structure of the signal, and from the results decides autonomously whether the object is friend or foe and decides what to do next. If enemy, The Solyaris applies electronic interference to shut down the data transmission channels and block the navigation and timing equipment. The complex has a modular design able to fit to specific battlefield environments.[121] The system is equipped with a radar and can defend an area of 80 square kilometers from UAVs. It disconnects the UAV from its command and control center and can work in a full automation mode without an operator's involvement. The Solyaris-mini is used to jam cellular communications and the Solyaris-keys defends against IEDs.[122]

Stupor—This electronic rifle suppresses communication channels and satellite navigation and blinds UAV optics. Its range is 600 meters with a 20-degree propagation zone. It paralyzes drones with between 4 and 25 seconds of irradiation, depending on the electronics of the drones' jamming resistance.[123]

Svet-KU—This is a system often associated with a separate Airborne Troops (VDV) formation. Specialists use the system to monitor the information environment and monitor various sources of radio signals. In automatic mode, the system monitors signals of various radio-electronic systems, analyzes them, and determines their coordinates at the source. It processes information in the frequency ranges from 25 megahertz to 18 gigahertz.[124] Guards Colonel Aleksandr Valitov, Commander of Airborne Troops 56th Guards Separate Airborne Brigade, stated that the Svet-KU is a mobile means of radio-technical control and protection of information against a leak over technical wireless communication channels. The system "makes it possible completely to block all communications at a distance, let us say, of 60 kilometers from this system and also to monitor them if necessary."[125]

Taran—This system repels swarm attacks with greater capabilities than the Pishchal. Installed on a tripod, it can cover defended facilities with a diameter of 2700 meters.[126] It is designed to detect and recognize hypothetical enemy communications assets such as radar stations, radio navigation, and radio-telecode systems.[127]

Tirada-2S—The system reportedly was detected in the Lugansk People's Republic. It is designed to disrupt the operation of telecommunications equipment and block operations of radar and electronic intelligence collection equipment.[128]

Torn—This system is used by Russian peacekeepers. It is an automated mobile reconnaissance system that helps to collect intelligence data in buffer zones and between opposing forces. It searches for signals in ranges up to 3000 MHz and can conduct

direction finding and source locations at a distance of up to 70 kilometers using the azimuth method.[129]
Zaslon-REB—This system was highlighted in 2017 and stated to be a smart control and monitoring complex that creates an "information security dome" over military forces. It can block unauthorized exchanges of information and jam signals of "all known mobile communication radio frequency bands," including GSM, LTE, CDMA, and Wi-Fi.[130] A day later an article appeared that stated the Zaslon's capabilities were overblown. Rather, its capabilities were stated to be extremely limited, since they only cover small facilities. Further, the article notes that many of the capabilities of the system were present in Soviet times and that they may have been "endowed with state-of-the-art technological properties" which appear modest at the moment.[131] It is unknown which description of the capability is more accurate.
Zhitel—The Zhitel automated jamming station combats UAVs at ranges of more than 20 kilometers. Crews in one exercise rehearsed the complete radio suppression of satellite and cellular communication stations that use the GSM and GPS standard, destroying the notional enemy's command-and-control system.[132] It can jam homing devices of cruise missiles and precision weapons,[133] and it fixes on and jams reconnaissance equipment on a UAV at any altitude and on any frequency band.[134] Zhitel can detect, get the bearings of, and jam satellite and cellular communication stations, and also satellite navigation systems (including GPS) over a radius of 20-30 kilometers.[135] It appears that Zhitel and Svet complexes are being used for defense from unmanned aerial vehicles in tandem. Zhitel jams in the radio frequency range, jamming cellular and satellite communications. For example, a drone could lose the connection with its operator and, depending on the software program that has been loaded into it, either lands or becomes totally unserviceable and crashes. Svet systems can precisely determine the location of the person controlling the drone. The complex conducts analysis and calculates the coordinates of the source of the signal of any electronic system. While Zhitel disables the control systems of unmanned aerial vehicles, Svet permits it to find who is controlling this vehicle. [136]

A:1.2 Aviation Complexes:

Name unknown—There was a report noting that electronic warfare systems have been developed for the Kh-101 (stealth air-to-surface cruise missile) and the Kh-102 (a nuclear version of the same cruise missile) cruise missiles that are carried by the Tu—22M3, Tu-95, and Tu-160 strategic bombers.[137]
Gimalai—This system is an updated version of the Khibiny. It is fitted to the Su-57 fighter. The system is fully integrated onboard and designed as a separate element of the aircraft's fuselage. The antenna system allows it to fulfill several functions at the same time: reconnaissance, REB, location, and so on. It can deliver active and passive jamming to the infrared seeker head of modern missiles and radars.[138]
Khibiny—This system is installed on the Su-34 front line bomber. It can create a false electronic situation. When it flew over the US Destroyer Donald Cook in 2014, it created electronic clones of additional targets. This meant that the destroyer's data and combat command and control weapon system were blocked as well. A new Khibiny-U system was attached beneath the wing at a suspension point and was developed for the Su-30SM.[139]
Rychag—This EW complex often on helicopters of the Mi-8MTPR-1 variety, can blind an enemy within a radius of several hundred kilometers and can suppress several targets at the same time. Such jamming causes enemy aviation intercept complexes to lose their capability to detect targets.[140]
Tarantul—This is a containerized system designed to protect the Su-34 and other aircraft. It is not certain, however, that the system ever reached the stage of implementation on any air frame.
Vitebsk—The complex can be adapted for any class of aircraft, to include military-transport and civilian aviation. The Su-25SM ground attack aircraft are equipped with this on-board complex. The export version is known as the President-S.[141] In Crimea, Russia turns on the Vitebsk REB jamming stations in its helicopters to preclude Ukraine's military, in Russia's estimation, from conducting an unauthorized launch against it.[142]

A:1.3 Naval Complexes:

MP-405—This complex can warn of detection and analyze and classify classes of illuminating electronic equipment and their carriers as to threat level. It can support the electronic suppression of all intelligence collection equipment and weapons.[143]

TK-25—This is the primary ship-based EW complex, according to the article. It supports the creation of pulsed disinformation and simulation jamming using digital copies of signals from the ships of all primary classes. It can analyze up to 256 targets simultaneously and support the protection of the ship.[144]

Author

Timothy Thomas is MITRE's EUCOM Information Operations Domain Specialist. He works with Fort Eustis and the Army's Future's Command as well on Russian and Chinese military issues, such as military thought, future war capabilities, and the information weapons that each country is developing. He is a former LTC in the US Army and is the author of eight books on Russian and Chinese military affairs.

About the Center for Technology & National Security

MITRE launched the Center for Technology and National Security (CTNS) to provide national security leaders with the data-driven analysis and technologically informed insights needed to succeed in today's hyper-competitive strategic environment. The Center aims to help policy-makers better navigate a dynamic, rapidly evolving technology landscape in order to advance U.S. interests and strengthen national security. As a part of the not-for-profit, non-partisan MITRE Corporation, CTNS is built on the experience and expertise of thousands of our nation's most respected scientific and engineering minds. The Center brings together experts and leading authorities from government, academia, industry, media, and policy institutes to drive informed discussion in this era of unprecedented technological change.

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.

Sponsor: US European Command
Dept. No.: P663
Contract No.: W56KGU-18-D-0004
Project No.: 0719S120

Endnotes

1 Russian sources and translators use the terms electronic warfare (EW and radio-electronic warfare (REB) interchangeably. Both terms are used as the appeared in various articles but have the same meaning.

2 Aleksandr Stepanov interview with Yuriy Illarionovich Lastochkin, "They Have Deployed a Dome, Which Defends from Missiles, Over the Russian Bases in Syria. Unique Electronic Warfare Systems, Which Are Capable of 'Blinding' Any Precision-Guided Weapon, Provide It," MK Online, 15 April 2018.

3 V. V. Selivanov and Yu. D. Ilyin, "Methodical Frameworks of Asymmetrical Response Formation in Military -Technical Struggles against a High-Technology Enemy," Military Thought, No. 2 2019, pp. 5-14.

4 Anatoliy Sokolov, "Umbrella Over Syria: Russian EW assets Confirmed High Effectiveness and Can Be Considered an Asymmetric Weapon for New-Generation Wars," VPK Voyenno-Promyshlenn Kuryer Online, 25 May-31 May 2016.

5 No author provided, "Deafening Success: EW System to Cover Europe from Near Kaliningrad," Izvestiya Online, 26 April 2019.

6 Aleksandr Kruglov and Nikolay Surkov, "Infantry Will Be Covered by an Electronic 'Umbrella': Electronic Warfare Battalions Will Appear in All Combined-Arms Armies," Izvestiya Online, 10 October 2018.

7 Ibid.

8 No author provided, "The Northern Fleet Completed Arming the Electronic Warfare (REB) Center," Izvestiya Online, 7 May 2019.

9 No author provided, "Central Military District Electronic Warfare Specialists Test New Way of Countering Enemy Airborne Assets," Ministry of Defense of the Russian Federation, 10 June 2019.

10 Aleksandr Sitnikov, "US for the First Time 'Shuts Down' Russian Electronic Warfare in Syria Account Published in America of New Method to Counter the 'Putin Threat,'" Svobodnaya Pressa, 18 October 2018.

11 Sergey Ishchenko, "Krasukha with Lysukha Have Struck Terror into NATO and Israel. A Norwegian Frigate on the Shoals, and the Iron Dome—Holes. Is this EW?" Svobodnaya Pressa, 13 November 2018.

12 Joe Gould, "Eyeing Russia, Lawmakers Aim to Boost Army Electronic Warfare," Defense News, 10 October 2017.

13 Roman Azanov, "With What Can Russia's Army 'Blind' and 'Suppress' an Enemy: The Automated Jamming Station from the 'Borisoglebsk-2' Electronic Warfare Complex," TASS, 15 April 2019.

14 Mike Eckel, "Ex-US Army Commander Warns of Russian Capabilities in Ukraine," Radio Free Europe, 24 January 2018.

15 Aleksey Ivanov, "Electromagnetic Bombs Created in Russia," Rossiyskaya Gazeta Online, 28 September 2017.

16 Oleg Bozhov, "We Have It! The Invisible Sword; Russia is Testing Electromagnetic Weapons That Burn the Insides of Enemy Missiles," Armeyskiy Standard, 12 October 2018.

17 No author provided, "Microwave Guns: Tests of New Weapons Have Started in the Russian Federation. Russia

Has Begun Field Tests of Electromagnetic Weapons," *Gazeta.Ru*, 1 October 2018.

18 Yuriy Lastochkin, interviewed by Viktor Khudoleyev, "Troops for the Battle in the Ether," Krasnaya Zvezda Online, 15 April 2014.

19 Ibid.

20 Yu. I. Lastochkin, "The Role and Place of Radio-Electronic Warfare Actions in Contemporary and Future Conflicts," Military Thought, No. 12 2015, pp. 14, 16.

21 Ibid., pp. 17-18.

22 No author provided, "Special EW Troop Range Will Be Established in Russia by 2018," RIA Novosti, 15 April 2016.

23 Oleg Falichev interview with Yuriy Lastochkin, "Dome over the Defense Ministry. Zaslon-REB System Blocks Any Channels of Information Leakage," VPK Voyenno-Promyshlennyy Kuryer Online, 26 April 2017-2 May 2017.

24 Ibid.

25 Ibid.

26 Ibid.

27 Gennadiy Miranovich interview with Yuriy Illarionovich Lastochkin, "On the Cutting Edge of Technologies: The Electronic Warfare Troops Are Celebrating Their Professional Holiday—15 April is Electronic Warfare Specialist's Day," Krasnaya Zvezda Online, 14 April 2017.

28 Yu. I. Lastochkin, Yu. L. Koziratsky, Yu. Ye. Donskov, and A. L. Mororescu, "Combat Employment of Radio-Electronic Warfare Troops as a Basic Component of Ground Forces Operational Art," Military Thought, No. 9 2017, pp. 18-25.

29 Ibid.

30 Ibid.

31 Ibid.

32 Ibid.

33 Unattributed author and title, Informatsionnyy Most, 9 August 2017.

34 Aleksandr Stepanov interview with Yuriy Illarionovich Lastohkin, "They Have Deployed a Dome, Which Defends from Missiles, Over the Russian Bases in Syria. Unique Electronic Warfare Systems Which are Capable of 'Blinding' Any Precision-Guided Weapon, Provide It," MK Online, 15 April 2018. Bold print did not appear in the original.

35 Vladimir Mukhin, "'Krasukha' Prevented the Tomahawks from Reaching the Targets. Russian Electronic Warfare Systems Successfully Underwent Baptism by Fire in Syria," Nezavisimaya Gazeta Online, 18 April 2018.

36 Yuriy Lastochkin, "EW Troops Guard the Airwaves. In the Realm of Information and Telecommunications, Supremacy Will Be with Us," Krasnaya Zvezda Online, 15 April 2019.

37 Aleksandr Pasmurtsev interview of Sergey Klindukhov, "The Strike Force of Netcentric Wars," Suvorovskiy Natisk, 26 April 2019.

38 Ibid.

39 M. Il'in, "Different Missions, One Goal," Armeyskiy Sbornik Online, No. 1 2019, pp. 30-33.

40 V. Khramov and A. Leontyev, "To Make an Operational Decision. The Intellectualization of the Electronic Warfare (EW) Command and Control Processes as One of the Primary Ways to Increase Its Effectiveness," Armeyskiy Sbornik Online, 31 May 2019.

41 V. A. Dvornikov, I. I. Korolev, and V. N. Pavlov, "On the Tactics of Electronic Warfare Forces," Military Thought, No. 3 2015, p. 10.

42 Ibid., p. 14.

43 Ibid., p. 10.

44 Ibid., p. 13.

45 Sokolov.

46 Yuriy Lastochkin, "Not a Day Goes by Without Interference: Electronic Warfare is Conducted Strictly According to Science," VPK Voyenno-Promyshlennyy Kuryer Online, 27 April 2016.

47 I. I. Korolyov, O. G. Nikitin, and S. N. Kozlitin, "Problems in Determining the Methods for Using the Forces and Means of Radio Electronic Warfare as an Arm of the Ground Forces," Military Thought, No. 9 2016, pp. 14-15.

48 Ibid., p. 15.

49 Ibid., p. 16.

50 Ibid., p. 17.

51 O. G. Nikitin, "Trends in Increasing the Effectiveness of the Organization of the Combat Employment of Radio-Electronic Warfare Troops in the Operations of Ground Forces Formations," Military Thought, No. 5 2017, p. 23.

52 Ibid., p. 24.

53 Ibid., p. 25.

54 Ibid., p. 27.

55 Ibid., p. 28.

56 Ibid., p. 29.

57 V. A. Orlov, Iu. N. Laygin, and D. M. Byvshikh, "Planning the Strategies for the Development of a System of Radio-Electronic Warfare Weapons," Military Thought, No. 5 2017, pp. 14-22.

58 Ibid.

59 Ibid.

60 Yu. Ye. Donskov, A. L. Morarescu, and P. N. Besedin, "Achieving Superiority in Command and Control as a Goal for the Use of Radio-Electronic Warfare Forces in Ground Force Operations," Military Thought, No. 1 2018, pp. 28-32.

61 No author provided, "Central Military District Electronic Warfare Specialists Disabled a Notional Adversary's Combat UAVs Outside Orenburg," Ministry of Defense of the Russian Federation (in English), 3 October 2018.

62 No author provided, "Eastern Military District Electronic Warfare Subunits in Buryatia Blocked the Operation of an Aggressor Communications Center," Ministry of Defense of the Russian Federation (in English), 15 April 2019.

63 "Eastern Military District…"

64 Ibid.

65 Roman Azanov, "With What Can Russia's Army 'Blind' and 'Suppress' an Enemy: The Automated Jamming Station from the 'Borisoglebsk-2' Electronic Warfare Complex," TASS, 15 April 2019.

66 No author provided, "Southern Military District Electronic Warfare Specialists Conducted Optical-Electronic Monitoring of the Forward Edge of the Aggressor's Defense in an Exercise in Stavropol Kray," Ministry of Defense of the Russian Federation, 15 April 2019.

67 No author provided, "Armenia to Get from Russia All Weapons on State Loan Before Year End—Armenian Defense

Minister," Interfax (in English), 2 October 2017.

68 No author provided, "Central Military District Electronic Warfare Specialists Ensure Armored Convoy's Safe Movement in Exercise Near Yekaterinburg," Ministry of Defense of the Russian Federation, 22 April 2019.

69 No author provided, "Electronic Warfare Subunits Near Orenburg Use Borisoglebsk-2 Complex to Jam the Communication Systems of a Notional Enemy," Ministry of Defense of the Russian Federation, 27 December 2018.

70 No author provided, "Central Military District's EW Specialists Prevent UAV Attacks on Command Post Using Borisoglebsk-2 System during Exercise in Orenburgskaya Oblast," Ministry of Defense of the Russian Federation, 18 March 2019.

71 No author or title provided, Ministry of Defense of the Russian Federation, 7 March 2019.

72 No author provided, "Bylina System RB-109A," TAdviser, 29 September 2017.

73 Aleksey Ramm, Dmitriy Litovkin, and Yevgeniy Andreyev, "Troops Will Get Electronic Warfare Artificial Intelligence System; Bylina System Will Independently Find, Identify, and Suppress Enemy Radar, Communications, and Satellites," Izvestiya Online, 4 April 2017.

74 No author provided, "Electronic Warfare Specialists Use Modern Dzyudoist System to Jam Signals of Guided Projectiles: After Using Radio Jamming to Suppress a Range of Frequencies and Disabling the Navigational Systems of Notional Enemy Drones at a Distance of More Than 50 Kilometers, Servicemen Prevent Drones from Approaching the Forward Edge of Their Troops," Zvezda TV Online, 8 July 2018.

75 No author or title provided, BBC Monitoring (in English), 3 February 2019.

76 Aleksey Kurilchenko, "The 'Eagle Owl' and 'Rook' Have 'Flown' to the Ships and Landed and Blinded All. Russia's Navy Begins to Take Delivery of the 5P-42 Filin Visual-Optical Jammer, Which Blinds the Enemy," Yezhenedelnik Zvezda, 12 February 2019.

77 Ibid.

78 No author provided, "Special Tactical Exercises with Electronic Warfare, Unmanned Aerial Vehicles Subunits Begin in Armenia," Ministry of Defense of the Russian Federation, 16 April 2019.

79 No author provided, "Russian Electronic Warfare Specialists Neutralize Radio-Controlled Minefields in Tajikistan Exercise," Ministry of Defense of the Russian Federation, 11 September 2018.

80 No author provided, "Central Military District EW Specialists in Tajikistan Learned to Cover a Vehicle Column from Enemy Precision-Guided Weapons," Ministry of Defense of the Russian Federation, 30 May 2019.

81 No author provided, "New Leer-2 Mobile Complexes Have Arrived at the Electronic Warfare Subunits of the Russian Military Base in Abkhazia," Ministry of Defense of the Russian Federation, 16 May 2017.

82 Nikolay Grishchenko, "Army Personnel Have Demonstrated Secret Electronic Warfare Equipment in Action Near Rostov," Rossiyskaya Gazeta Online, 25 August 2018.

83 No author provided, "Smart UAVs Protect Peacekeepers Engaged in Separating Conflicting Sides," Ministry of Defense of the Russian Federation, 23 August 2018.

84 Aleksey Ramm and Vladimir Zykov, "The Russian Army Has Obtained a Cellular Weapon: The Modernized Leer-3 Complex Will Be Able to Send Instant Messages and Audio and Video Messages," TASS, 25 January 2017.

85 "Central Military District Electronic Warfare Specialists Ensure…"

86 No author provided, "In Amurskaya Oblast Electronic Warfare Specialists Defend Military Vehicle Convoys during a March against Combat Drone Attacks by Setting Up a Defensive 'Radio Dome,'" Ministry of Defense of the Russian

Federation, 18 April 2019.

87 No author provided, "Eastern Military District Unmanned Aerial Vehicle Combat Composite Detachment Provides Cover for Artillery Operations during an Exercise in Priamur'ye," Ministry of Defense of the Russian Federation, 23 October 2018.

88 No author provided, "Brand-New Lesochek Electronic Warfare Systems Delivered to the Western Military District Tank Army," Ministry of Defense of the Russian Federation, 5 December 2018.

89 No author provided, "Training Assemblies with Electronic Warfare Specialists Are Occurring in the Western Military District," Ministry of Defense of the Russian Federation, 22 November 2017.

90 No author provided, "Southern Military District Electronic Warfare Specialists Conduct Electronic Countermeasures against Notional Enemy in the Mountains of Dagestan," Ministry of Defense of the Russian Federation, 8 October 2018.

91 No author provided, "Southern Military District Electronic Warfare Specialists Held a Special Tactical Exercise in Communications Jamming of a Simulated Enemy in the Mountains of Dagestan," Ministry of Defense of the Russian Federation, 25 August 2018.

92 Anton Valagin, "The Electronic Troops Switched Off a Flying Radar Near Kursk," Rossiyskaya Gazeta Online, 9 October 2018.

93 Aleksey Ramm, Bogdan Stepovoy, and Aleksey Kozachenko, "Electronic Shield: Defense Ministry Deploying Electronic Warfare Resources in Syria. New Systems Already Delivered to Humaymim Airbase," Izvestiya Online, 25 September 2018.

94 "Central Military District Electronic Warfare Specialists Ensure…"

95 No author provided, "Troops Being Equipped with New Jammers," Rossiyskaya Gazeta Online, 16 April 2019.

96 No author provided, "Russia May Supply Syria with Krasukha-S4 EW Systems, Zhitel Radar-Jamming Stations," Interfax (in English), 28 September 2018.

97 Roman Azanov, "With What Can Russia's Army 'Blind' and 'Suppress' an Enemy: The Automated Jamming Station from the 'Borisoglebsk-2' Electronic Warfare Complex," TASS, 15 April 2019.

98 No author provided, "Central Military District EW Specialists Conducted an Electronic Strike Against the Aggressor's Communications Centers during the Course of an Exercise in Yekaterinburg," Ministry of Defense of the Russian Federation, 25 April 2019.

99 No author provided, "The Northern Fleet Completed Arming the Electronic Warfare (REB) Center," Izvestiya Online, 7 May 2019.

100 No author provided, "Russia Is Deploying the Murmansk-BN Electronic Warfare System to the Kaliningrad Region," Izvestiya Online, 26 April 2019.

101 "Deafening Success…"

102 No author provided, "The Northern Fleet Has Completed Its New Center for Radio-Electronic Warfare," Kirkenes The Independent Barents Observer (in English), 21 May 2019.

103 No author provided, "Central Military District Artillery Formations Acquire First Separate UAV Subunits," Ministry of Defense of the Russian Federation, 13 March 2019.

104 No author provided, "First Palatin Radio Electronic Warfare System in the Russian Armed Forces Arrives in the Western Military District Combined-Arms Army Troops," Zvezda TV Online, 10 April 2019.

105 Vladimir Tuchkov, "Russia Has Opened the Hunting Season on Unmanned Aerial Vehicles. 'Taran,' 'Sapsan,' and 'Solyaris-N' Have Learned to Strike Enemy Drone Swarms," Svobodnaya Pressa, 1 November 2018.

106 No author provided, "Pole-21 Systems for Countering Drones Control Systems to Be Put into Service in Central Military District for the First Time," Interfax (in English), 15 Aril 2019.

107 Vladimir Tuchkov, "Russia Has Opened…"

108 No author provided, "During Exercise in Buryatiya Eastern Military District Electronic Warfare Subunits Disrupt Troop Command and Control System of Notional Adversary," Ministry of Defense of the Russian Federation, 27 December 2018.

109 No author provided, "Central Military District Electronic Warfare Subunits in Siberia Receive Newest Rtut-BM System," Yekaterinburg Ural'skiye Voyennyye Vesti, 8 May 2019.

110 No author provided, "EW Specialists Placed Command Post Under Protective Dome during Exercise in Kemerovskaya Oblast," Ministry of Defense of the Russian Federation, 19 March 2019.

111 No author provided, "Central Military District EW Subunits in Siberia Receive Newest Rtut-BM System," Ministry of Defense of the Russian Federation, 13 March 2019.

112 No author or title provided, Minsk Salidamasts, 29 October 2018.

113 No author or title provided, Zvezda TV, 28 October 2018.

114 Vladimir Tuchkov, "Russia Has Opened…"

115 Ibid.

116 Pavel Kutarenko, "'Serp' System: Staff Testing of a New Hunter of Unmanned Vehicles," Zvezda TV Online, 30 April 2019.

117 Tuchkov.

118 No author provided, "Western Military District Electronic Warfare Subunits Use Silok to Bring Down 'Terrorist' Unmanned Aerial Vehicle's in Leningradskaya Oblast," Ministry of Defense of the Russian Federation, 2 November 2018.

119 No author provided, "Silok Systems Used for First Time to Intercept Enemy Unmanned Aerial Vehicles in CSTO Exercise," Ministry of Defense of the Russian Federation, 2 November 2018.

120 Pavel Nastin, "This Has Never Happened Before: Brilliant Premieres at Vostok-2018 Exercises. During the Maneuvers Our Servicemen Had to Perform Certain Combat Training Tasks for the First Time," Zvezda TV Online, 13 September 2018.

121 Aleksandr Khokhlov, "Like a Combat Laser at Flying Iron: The Top Five Russian Anti-UAV Weapons. Russia's Armed Forces Now Have the Means to Counter Any Type and Make of Potentially Hostile Drone," Yezhenedelnik Zvezda, 15 November 2018.

122 Vladimir Tuchkov "Russia Has Opened…"

123 Ibid.

124 No author provided, "Separate VDV Formation in Volgograd Oblast Receives Unique Mobile Radio-Electronic Warfare System," Ministry of Defense of the Russian Federation, 29 June 2017.

125 "Military Council" interview with Guards Colonel Aleksandr Valitov, Commander of the Airborne Troops 56th Guards Separate Airborne Brigade, by Anatoliy Yermolin, no title provided, Ekho Moskvy Online, 1 July 2017.

126 Vladimir Tuchkov, "Russia Has Opened…"

127 No author provided, "Central Military District Electronic Reconnaissance Specialists Intercept Hypothetical Enemy Radio Signals in Exercise in Southern Urals," Ministry of Defense of the Russian Federation, 10 January 2019.

128 No author provided, "Ukraine Announced Detection of the Latest Russian Electronic Warfare Equipment," Avia.pro, 24 March 2019.

129 No author or title provided, Ministry of Defense of the Russian Federation, 23 May 2019.

130 Aleksey Ramm and Vasilisa Belokopytova, "Military Units Have Been Sealed Off by the Impenetrable 'Zaslon'," Izvestiya Online, 19 April 2017.

131 Aleksandr Sharkovskiy, "The Modest Potential of the 'Zaslon-REB' Complex. The Capabilities of the New Information Security System Are Extremely Limited," Nezavisimaya Gazeta Online, 20 April 2017.

132 No author provided, "Electronic Warfare Specialists Practice Suppression of Notional Enemy Unmanned Aerial Vehicles Near Chelyabinsk," Ministry of Defense of the Russian Federation, 27 June 2018

133 No author provided, "Special Groups for Combatting UAVs Created in All Central Military District Formations," Ural'skiye Voyennyye Vesti, 6 July 2018.

134 No author provided, "Newest Counter-UAV Complexes Will Be Employed for the First Time in the Vostok-2018 Maneuvers," Ministry of Defense of the Russian Federation, 12 September 2018.

135 "Electronic Shield: Defense Ministry…"

136 Timofey Borisov and Sergey Ptichkin, under the rubric, "The Army": "A Radar Field Will Defend Russian Cities from Unmanned Aerial Vehicles," Rossiyskaya Gazeta Online, 23 June 2018.

137 No author or title provided, RIA Novosti, 9 November 2018.

138 Roman Azanov, "With What Can Russia's Army 'Blind' and 'Suppress' an Enemy…"

139 Ibid.

140 Ibid.

141 Ibid.

142 No author provided, "Helicopters of the Russian Federation Aerospace forces in Crimea Turn on Electronic Warfare Stations Due to Threats of Provocation on the Part of Ukraine," RIA Novosti, 4 June 2019.

143 Azanov.

144 Ibid.

MITRE Center for Technology and National Security