From the JED Archives: Tuning in, Turning on: Russia Brings Radio-Electronic Combat to the Fore

By Richard Scott

While the western media has in recent years made much of the Kremlin's investment in advanced kinetic capabilities – notably hypersonic missiles, new strategic weapons, a nuclear-powered cruise missile, nuclear-armed torpedoes and laser weapons – it has given far less attention to another area of warfare where the Russian military poses an increasing challenge to the US and its NATO allies. Operations over the past decade have served to demonstrate the importance Russia attaches to electronic warfare (EW) – or radio-electronic combat (*radioelektronnaya borba – REB*) – as an intrinsic part of its military doctrine.



Russian MOD

Fortunately, the reinvigoration of Russian EW – and its implications for military thinking across the NATO alliance – have not gone unnoticed by strategic think tanks and research institutes in the west. Recent studies in the unclassified realm, based on extensive surveys of open source literature, have provided valuable insights into how both political and military leadership in Russia has come to embrace REB as an enabler and a force multiplier.

Russian operations in eastern Ukraine and Syria since 2015 have enabled specialist EW ground force units to put theory into practice. The application of REB in these campaigns – in support of both kinetic and non-kinetic operations – has provided NATO with a very real and immediate demonstration of the importance of EW in a "hybrid" battlespace, and highlighted significant gaps in the Alliance's own capabilities.

During the Cold War, NATO recognized the criticality of EW supremacy and, conscious that any confrontation with Warsaw Pact forces would almost certainly be in a dense and hostile Electromagnetic Operational Environment (EME), invested accordingly in doctrine, equipment and training. The potency of this capability was demonstrated to great effect in 1991, as a US-led coalition air campaign systematically blitzed Iraqi air defenses.

However, the two decades of "violent peace" that followed the fall of the Berlin Wall saw the Alliance's EW capabilities and doctrines steadily atrophy. With no peer competitors to speak of, US forces and its NATO partners largely found themselves involved in counter-insurgency, crisis response and peace support operations in which they enjoyed a significant technological advantage. Adversaries, such as Serbia,

Afghanistan and Libya, were equipped with aging and degraded integrated air defense systems, few (if any) naval defenses and a very limited ability to challenge NATO ground forces. From a threat perspective, this enabled NATO forces to operate in very permissive air, ground and naval environments.

As a result, NATO's EW focus during operations in Afghanistan and Iraq, for example, was largely confined to aircraft self-protection against IR-guided man-portable air defense systems (MANPADS) and protecting ground forces against remotely controlled improvised explosive devices (RCIEDs). All the while, the use of the EME for sensing, communications, navigation and targeting was becoming steadily more important to NATO forces. To this end, unhindered access to the EME became something of an article of faith rather than a strategic imperative.

"Moscow's interest in boosting EW capabilities vis-à-vis NATO has its origins in seeking to asymmetrically challenge the alliance on Russia's periphery and maximise its chances of success in any operation against NATO's eastern members" – Roger McDermott.
Over the past decade, the return to great power competition, and particularly the resurgence of Russia as a military power, has forced NATO and other western militaries to confront a new set of challenges in the EME. Indeed, it is widely argued that Russia's EW strategy is an integral component of a wider anti-access/area denial (A2/AD) strategy that puts NATO's frontline states at risk.

This concern was front and center of Roger N. McDermott's report, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*.[Display footnote number:1] Published in 2017 by the Tallinn-based International Centre for Defence and Security in conjunction with the Estonian Ministry of Defence, the study outlined the scale of Russian EW investments in the context of its wider military capabilities, examined the organizational structure of its REB

forces, and considered the practical implications for NATO's eastern flank using evidence from Russia's use of EW in recent conflicts.

"Moscow's interest in boosting EW capabilities vis-à-vis NATO has its origins in seeking to asymmetrically challenge the alliance on Russia's periphery and maximise its chances of success in any operation against NATO's eastern members" writes McDermott in the report's introduction. "Russia has consistently invested in EW modernisation since 2009, with modernised EW systems entering service across strategic, operational and tactical levels to augment capabilities of all service branches and arms."

He continues: "Modernisation of the EW inventory is set to continue in the State Armaments Programme up to 2025, which means Russia's military will benefit greatly from further advances in EW capability."

ASYMMETRY

For Russia, the big attraction of EW is its asymmetric impact in the face of Western technological supremacy. "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 [of] attacking frequencies," says Timothy Thomas in his introduction to MITRE's September 2020 report, *Russia's Electronic Warfare Force: Blending Concepts with Capabilities*.[Display footnote number:2] He goes on to describe how Russian EW practitioners seek a targeted and coordinated electronic blizzard to degrade sensors and communications, and so induce "disorganization" in adversary command and control.

This broad theme was also expounded in the American Security Project's (ASP's) April 2020 report, *Russian Electronic Warfare: A Growing Threat to US Battlefield Supremacy*, in which author Patrick Smith argues that Russia's investment in

REB attempts to level up the technical superiority enjoyed by the United States – and by definition its NATO partners – in command, control, communication, computers and intelligence (C4I).[Display footnote number:3] "EW can target communications the US uses to coordinate operations in multiple domains, or it can disrupt or degrade the navigation systems used by US forces to locate themselves and identify targets for precision guided munitions," he writes, adding: "In a struggle against a highly advanced foe like NATO, EW could help to level the playing field. Indeed, Russia's interest in boosting its capabilities originated in an effort to asymmetrically challenge the more vulnerable member states on the alliance's periphery and maximize the chances of success in an operation against eastern NATO members before the alliance could organize a coordinated response."

Smith also sets the contribution of EW in the wider context of psychological operations (psyops) and cyber warfare. "The adage holds that armies march on their stomachs, but, today, modern militaries rely just as much on data feeds," he suggests. "In this environment, Russia thinks EW can play an integral role in a holistic approach to warfighting."

REB REGENERATION

While President Vladimir Putin had endorsed a long-term EW strategy and policy document as far back as 2002, most analysts trace the regeneration of Russian EW capability back to 2008, when the poor performance of forces and equipment in Georgia drove the Kremlin to launch major reform and modernization of the military. Since then, there have been sweeping changes to the training, force structure and integration of EW forces, and a substantial modernization of equipment capability (most notably in the ground forces).

In the Swedish Defence Research Agency's (FOI's) September 2018 report, *Russian Electronic Warfare: The Role of*

Electronic Warfare in the Russian Armed Forces, author Jonas Kjellén points out that the formation of the EW Troops in 2009 was critical in that it elevated the status of the branch to that of other combat support arms.[Display footnote number:4] "The immediate and probably single most important result of this was the formation of a headquarters for the EW commander within the General Staff," Kjellén says. "Since 2009, this enlarged EW command structure has been essential for the general development of Russian EW forces. It has enhanced coordination within the EW domain, provided better means of integration with other force structures and facilitated the comprehensive rearmament programme."

McDermott's earlier study detailed the transformation of Russian EW forces between 2009 and 2015, with previously disparate EW units spread throughout the military being reorganized at operational and strategic levels into brigades. "As a result, Russia currently has five EW brigades across its Military Districts, with two located in Western Military District – though this may well change in the future as demand for EW capacity increases," says McDermott. "Each of these brigades consists of four EW battalions and one company."

He continues: "Russia's most powerful EW systems—such as the Krasukha, Leer-3, Moskva and Murmansk-BN—are located in the Ground Forces' EW brigades; these systems offer ranges of several hundred kilometres. These brigades are tasked with providing combat support to the manoeuvre brigades, and can be broken down into smaller parts depending on the size of force and type of mission for which it is tasked."

Organizational change has been accompanied by significant investment in modernized equipment, says Kjellén. "Since 2009, new EW units have been formed, a large number of new EW systems have been procured, and new roles and tasks have been given to the EW Troops. Taken together, these form the 'new look' of Russian EW capabilities which has been

enthusiastically propagated by members of the Russian EW community."

The last decade has also seen a significant recapitalization to upgrade the EW equipment inventory. "Not only have new pieces of EW equipment been procured in large numbers, but the number of different systems and complexes developed is also high," observes Kjellén in his FOI study. "In an interview in 2014, the EW commander [Major General Yuriy Lastochkin] disclosed that 18 new EW complexes had completed state trials in the period 2010-2013, 14 of which were mentioned by name: the Borisoglebsk-2, Alurgit, Infauna, Krasukha-2O, Krasukha-S4, Moskva-1, Parodist, Lorandit-M, Leer-2, Leer-3, Lesochek, Less, Magnii-REB and Pole-21.

"In addition to these 14 complexes, around ten new complexes have completed state trials since 2013, or are as yet unfinished projects that are publicly known about. It is also quite possible that recently fielded EW equipment exists that is not known about for reasons of greater secrecy or because numbers are low."

FOI's report also draws attention to the importance attached to command and control of EW complexes. "The main purpose is to increase the combat efficiency of EW units through information sharing and automated processes, but the aim is also to increase coordination of surveillance in the [electromagnetic spectrum] in peacetime," writes Kjellén. "This is an area that relies on technological capacities to create and field such EW command and control systems, but it is largely also an organizational issue that implies closer interaction among EW assets at different levels of subordination."

He adds: "The EW command and control systems will also be able to feed into, and retrieve information from, the non-EW command and control systems within the different branches of service and independent combat arms."

Another important waypoint in the regeneration of Russia's EW capability was a consolidation of the military industrial complex in 2009. This saw a number of companies brought under the umbrella of a single holding company known as JSC Concern Radio-Electronic Technologies (Kontsern Radioelektronnye Tekhnologii – KRET). A member of the State Corporation Rostec, KRET today has over 70 member companies, employing over 50,000 staff across Russia, engaged in engineering and manufacture of electronic systems for military, aerospace and civil markets.

PROVING GROUND

Russia's annexation of Crimea, and operations in the Donbass region of Ukraine, have offered an insight into Russia's employment of EW in a contemporary warfare environment. Indeed, the conflict in eastern Ukraine has been frequently described as a proving ground for Russian ground-based EW capability.

In his recent ASP report, Smith highlights how EW had been used to support kinetic operations in Ukraine, noting that "Russia has managed to disrupt the Ukrainian military's communications equipment [forcing] Ukrainian soldiers to rely on their cellphones to communicate." Furthermore, while Russia uses EW to jam some communication, "it also used EW tools to intercept enemy communications and triangulate Ukrainian forces to target them with rocket artillery."

Effective application of EW also managed to turn some technology used by the Ukrainians against them. "Due to jamming and hacking, Ukrainian forces found US supplied Raven RQ-11B drones more of a liability than an asset," says Smith. "An advisor to the Ukrainian military noted the drones were no longer in use on the front lines because, among other things, they allowed the enemy to see Ukrainian military positions." Russia has also used EW as a tool in support of psychological operations, identifying Ukrainian military personnel through

their cellphones and then sending intimidating text messages.

It is also no secret that the Organization for Security and Cooperation in Europe (OSCE) Special Monitoring Mission to Ukraine (SMM) has frequently found its UAV-based airborne surveillance operation disrupted by hostile jamming. As a result, some of the Scheibel S-100 Camcopters used by the OSCE SMM have crashed, while others have entered auto-return mode. In other cases, Camcopter missions have been disrupted by GPS jamming.

McDermott's ICDS study digs deeper into the Russian employment of REB in Ukraine. He points out that while much of the Russian EW activity in the Donbas region was clandestine – given that it was being undertaken in support of separatist elements – there is no doubt that it has allowed the Russian military to gain vitally important experience in exploiting EW assets in a range of operational settings. He identifies a number of use cases: EW to target Ukrainian unmanned aerial systems by jamming control links or GPS signals; electronic countermeasures to disrupt electronically-fused munitions fired from artillery and mortars; the disruption and degradation of enemy communications such that there were localized blackouts; and the detection and geo-location of electromagnetic emissions to support counter-targeting.

Russia has deployed both in-service EW systems and new equipment undergoing trials into theater. Based on open sources and his own interviews, McDermott's report identifies a number of novel aspects to operations. For example, the use of highly mobile tactical EW groups constantly changing location to avoid destruction under fire, and experimentation with new EW algorithms. However, he saw the chief innovation being the much larger scale use of EW in support of operations, with the Russian General Staff apparently assigning considerable importance to the testing of new tactics, and evaluating the effectiveness of automated and mobile systems.

The ICDS report also refers to two occasions during the Ukraine conflict when Russian units and equipment intervened directly to support separatists. “These were marked by typical combined-arms approaches to warfare,” says McDermott, “and in each case, Russian and proxy forces quickly secured local victory. However, also present in each instance were EW assets and the use of EW in preparing, conducting and completing the local operation.”



Russia places significant emphasis on training its EW operators. RUSSIAN MOD

The first instance, in August 2014, was in Ilovaysk, located 25 km east of Donetsk. In this case, says McDermott, “a series of kinetic contacts precipitated the encirclement of Ukrainian forces by Russia’s Armed Forces units from Pskov and Kursk; this involved the deployment of battalion tactical groups, reconnaissance and sabotage groups including EW units, transferred from Russian territory to the conflict zone. Ahead of the engagement, EW assets were also arriving in the area in preparation for the ensuing operation; these were to be used to suppress enemy communications.”

Systems deployed included Leer-2, Rtut-BM and Lorandit (to intercept, geo-locate and jam GSM networks), Krasukha-2 and Krasukha-4 (for suppression of hostile surveillance/fire control radars) and Borisoglebsk-2 (designed to disrupt C2 networks). Russian EW assets were tasked with suppressing

radio communications at tactical and operational levels, fixing and locating enemy forces by identifying EMS usage, disrupting C2, blocking mobile phone networks, and spreading false information as part of psyops.

McDermott highlights two particularly important areas of Russian EW use in Ilovaysk: fixing and targeting for artillery; and the complementary exploitation of EW to facilitate psyops. “Russian EW systems would detect enemy communications transmissions, including mobile phones, to provide target information to conduct artillery strikes. Moreover, by disrupting [the] enemy’s mobile networks and transmitting data, some instances involved Ukrainian personnel receiving negative text messages on their phones, aimed at undermining morale. Such psyops and EW integration may not have been on a wide scale, but it certainly took place sporadically and among significant numbers of [Ukrainian] personnel.”

The second case of direct support occurred in January-February 2015, when the area around Debaltseve witnessed a surge in fighting. “As in Ilovaysk, Russian EW systems were deployed in advance to prepare the battlefield and during the combat operations,” said McDermott. What differed on this occasion was the use of a comprehensive technical EW monitoring group tasked with monitoring the EMS, apparently using the experience gained earlier in Ilovaysk. “EW assets were deployed by Russia’s armed forces for direction-finding/geo-location, disrupting enemy communications among other features. This also used automated jammers,” he writes.

According to McDermott, the overall scheme of EW operations implemented a highly automated degree of spectrum monitoring, interception, jamming and intelligence analysis, working closely with SIGINT and providing information in real time. “Russian groups again used EW systems, most likely Leer-3, to facilitate psyops…with numerous reports of Ukrainian military servicemen receiving text messages aimed at undermining their

morale. Likewise, the high level of accuracy in artillery fire stemmed from successful employment of EW to fix and locate enemy targets by identifying mobile phone emissions in communications between [Ukrainian] servicemen," he writes, adding: "The importance of Russian EW in these kinetic operations in Ukraine offers deeper insight into how such assets will be exploited in future conflict."

While President Vladimir Putin had endorsed a long-term EW strategy and policy document as far back as 2002, most analysts trace the regeneration of Russian EW capability back to 2008, when the poor performance of forces and equipment in Georgia drove the Kremlin to launch major reform and modernization of the military.
McDermott concluded that Russia's military involvement in the Donbas region, more than any previous conflict, provided not only valuable opportunities for experimentation "but also marked a closing of the gap between the theory underlying EW and its application in support of combat operations." This ranged from "warping information in support of psyops, to jamming, blocking and disrupting the adversary's communications and radars, and disorganising the enemy's ability to conduct C2 during operations."

CONCLUSIONS

There is a broad consensus that NATO must sit up and take notice of how Russia's revitalized EW capabilities have fundamental and long-term implications for NATO. That said, analysts also voice caution regarding the true nature of the threat, pointing out that Russian media is prone to over-exaggerate the performance of domestic systems.

For example, Kjellén points out the difficulties in accurately assessing Russian EW capabilities. "Much of EW is often shrouded in military secrecy, and the often complex technological nature of EW breeds misconceptions that occasionally create and fuel myths," he writes. "The

deterioration in relations between Russia and the West, involving both deliberate Russian disinformation and a 'Russia scare', has added to this problem."

However, Kjellén suggests that changes in organization support the view that EW now enjoys higher in status in Russian military thinking. "The formation of EW Troops is the most important factor, but the weight of EW in the Russian armed forces has also generally increased. There are now larger and more capable EW sub-units in both the Ground Forces' and the Airborne Troops' major combat formations.

"Denying a high-tech adversary the ability to make use of its command and control system undisturbed is now perceived as crucial to modern warfighting, at both the tactical and the operational level. Moreover, the creation of large EW formations and an expanded EW command structure represent an unprecedented capability for the Russian Armed Forces to conduct EW combat support operations at the theater level."

MITRE's report also identifies the targeting of NATO C2 as a priority for Russian EW forces given the impact this could have on decision-making. According to Thomas, while the West worries about Russian A2/AD 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." He continues: "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."

In his ICDS report, McDermott argues that Russia's exploitation of EW assets in support of operations in south-eastern Ukraine "offers very limited lessons for NATO as such, since the alliance can field advanced technological assets way beyond anything that [Ukraine] can bring to bear.

“Moreover,” he adds, “some Russian claims to be able to completely technologically degrade the EMS are palpably false.”

That said, McDermott fully acknowledges that, through force multipliers such as EW, the continued transformation of the Russian armed forces “will offer a conventional capability way beyond that possessed by the Soviet legacy force” at the end of the Cold War. He continues, “If conflict with Russia ever erupts on NATO’s Eastern Flank, the first sign of activity will be in the EMS – and in this spectrum the initiative and advantage will be determined.

“Moscow appears to perceive this as an area of possible weakness on the part of the alliance, and has therefore invested in further strengthening this capability. This means that NATO must change its approaches to policy, doctrine, organisation, capabilities, training, tactics and procedures, and exercise scenarios.”

REFERENCES

1. Roger N. McDermott, Russia’s Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum, International Centre for Defence and Security, September 2017.
2. Timothy Thomas, Russia’s Electronic Warfare Force: Blending Concepts with Capabilities, MITRE Center for Technology and National Security, September 2020.
3. Patrick Smith, Russian Electronic Warfare: A Growing Threat to US Battlefield Supremacy, American Security Project, April 2020.
4. Jonas Kjellén, Russian Electronic Warfare: The role of Electronic Warfare in the Russian Armed Forces, FOI September 2018.