ADAPTING TO THE SPECTRUM:

Operating in the EMS Domain in the European Theater

Ryan Mendenhall, Major, USAF
Melissa Crenshaw, Major, USAF
Anthony Mafnas, Major, USAF
William Dean Long, Major, USMC

WRIGHT FLYER PAPERS

Air Command and Staff College

Col Benjamin B. Hatch, Commandant
Dr. Heather Venable, Director of Research and Chair of the Wright Flyer Selection Committee
Dr. Stephanie Hinnershitz, Lt Col Kristi Buczek,
Lt Col Garick Chamberlain, Dr. Jon Hendrickson

Please send inquiries or comments to

Editor
The Wright Flyer Papers
Department of Research and Publications (ACSC/DER)
Air Command and Staff College
225 Chennault Circle, Bldg. 1402
Maxwell AFB AL 36112-6426

Tel: (334) 953-3558
Fax: (334) 953-2269

Email: acsc.der.researchorgmailbox@us.af.mil

AIR UNIVERSITY

AIR COMMAND AND STAFF COLLEGE

Adapting to the Spectrum:

Operating in the EMS Domain in the European Theater

Maj Ryan Mendenhall, USAF; Maj Melissa Crenshaw, USAF;
Maj Anthony Mafnas, USAF; Maj William Dean Long, USMC

Wright Flyer Paper No. 100

Air University Press
Maxwell Air Force Base, Alabama

Commandant, Air Command and Staff College
Col Benjamin B. Hatch

Director, Air University Press
Patrick J. Charles

Project Editors
Dr. Achala Gunasekara-Rockwell
Kimberly Leifer

Cover Art, Book Design, and Illustrations
Catherine Smith

Composition and Prepress Production
Jonathan Marks

Accepted by Air University Press in December 2025 and Published August 2026

ISSN 2687-7260

Air University Press
600 Chennault Circle, Building 1405
Maxwell AFB, AL 36112-6010
https://www.airuniversity.af.edu/AUPress/

Facebook:
https://facebook.com/AirUnivPress

X:
https://x.com/aupress

LinkedIn:
https://www.linkedin.com/company/air-university-press/

Instagram:
https://www.instagram.com/air_university_press/

Disclaimer

AIR UNIVERSITY PRESS

Contents

Foreword *iv*

Abstract *v*

Introduction **1**

Observed System **1**

Desired System **12**

Problem Sets **13**

Operational Approach **14**

LOE 1: NATO Electronic Protection Measures and Maneuverability in EMS **15**

LOE 2: EW Usage to Degrade Russian Ground Forces **17**

LOE 3: Identifying and Countering Russian Offensive EW **18**

Conclusion **20**

List of Acronyms **24**

Bibliography **26**

Foreword

The Wright Brothers remind us that transformative military capability begins with bold ideas, disciplined experimentation, and the courage to rethink what is possible. The Wright Flyer series continues that tradition of intellectual innovation. From the Air Corps Tactical School's pioneering concepts on strategic airpower to the Manhattan Project's fusion of science with a warfighting strategy, airpower history demonstrates that rigorous research is not academic luxury—it is a warfighting imperative. Breakthroughs occur when professionals challenge assumptions and interrogate complex problems, pushing past traditional limiting boundaries. When we invest in deliberate inquiry, we expand the range of strategic and operational options available to commanders and national leaders.

ACSC students stand in that lineage. They are not merely learning about warfighting—they are actively shaping its future. Their scholarship informs doctrine, drives capability development, and anticipates the demands of tomorrow's contested environments. The Wright Flyer series is both a platform and a charge: to think critically, innovate boldly, and produce work that meaningfully enhances the effectiveness of the joint force. Through purposeful research, we ensure airpower's continued ability to deliver solutions to political objectives.

At ACSC we not only educate to win, but we also research to sustain decisive joint warfighting advantages.

BENJAMIN B. HATCH
Colonel, USAF
Commandant

Abstract

Russia continues to threaten European security as it modernizes its military and demonstrates a willingness to challenge international sovereignty. It is fielding sophisticated electronic warfare systems capable of disrupting North Atlantic Treaty Organization command and control, denying Global Positioning System access and space-based intelligence, surveillance, and reconnaissance capabilities, and jamming the communications required to conduct military operations. These developments pose one of the most consequential yet understudied challenges to NATO deterrence and defense against future Russian aggression. In part, this challenge stems from the alliance's lagging development of electronic protection measures against Russian electronic warfare capabilities and its lack of preparedness to operate in a contested electromagnetic spectrum environment. This paper first analyzes the observed system using operational design methodology to assess the current operating environment. It then evaluates the desired system and end state to identify the barriers and problem sets NATO must overcome to achieve its objectives. Finally, it recommends an operational approach built around three lines of effort to establish electromagnetic spectrum superiority in a conflict between NATO and Russia.

Introduction

Observed System

Understanding the current operating environment is essential to identifying the conditions that shape a potential conflict between NATO and Russia. This section examines the observed system by analyzing the operational environment, the role of the EMS, Russian EW capabilities, and the critical dependencies that enable NATO operations. Together, these factors reveal the vulnerabilities, constraints, and competitive dynamics that will influence the ability of either side to gain and maintain an advantage in the EMS domain.

Operational Context and EMS Domain

The most likely scenario of a conflict between NATO and Russia is one in which Russia continues its revisionist approach to use military forces to reclaim states that were part of the former Soviet Union. Russian actions in Georgia, Moldova, and Ukraine demonstrate Russian President Vladimir Putin's willingness to violate international sovereignty and highlight the threat posed to the NATO territories such as Poland and the Baltic states of Lithuania, Latvia, and Estonia. Russian military planners recognize their strength lies in employing overwhelming numbers of motor-rifle brigades and artillery ground units to rapidly advance across a front to seize terrain before the adversary can react.

NATO does not maintain the numerical ground force posture to stop a Russian invasion and relies on NATO air and maritime power to attrit the enemy. Russian fielding of A2/AD systems, comprising multiple layers of air and missile defense systems, can keep NATO assets at range. Additional Russian EW capabilities enhance the anti-access/area denial (A2/AD) by degrading NATO command and control, intelligence, surveillance, and reconnaissance (C2ISR); air and maritime asset communication; and prevent standoff munition terminal guidance by denying EMS access. Russia is also vulnerable to similar EMS denial capabilities, and a mutually denied EMS environment is a realistic possibility.

JADOs are essential for defeating a near-peer adversary such as Russia, but they depend on access to the EMS. While establishing "EMS supremacy" is the most desirable, it is likely unrealistic or not operationally feasible to achieve. This paper recommends "EMS superiority" as the appropriate range of EMS control.

Air Force Doctrine Publication (AFDP) 3-85, *Electromagnetic Spectrum Operations (EMSO)* defines EMS superiority as "secure, reliable conduct of operations at a given time and place in the EMS without prohibitive interference from the opposing force. EMS superiority may be managed by location, system, frequency, and time. Commanders should determine the minimum level of EMS control required to accomplish their mission and assign an appropriate level of effort to achieve it."[1]

The team that can successfully establish access and maneuver within the EMS domain will maintain a positional advantage throughout the conflict.

EMS Maneuver

To gain superiority in the EMS domain, NATO and the US must understand how to maneuver in the EMS space. Maneuver, as described in Joint Publication 3-0 *Joint Operations*, is "the employment of forces for offensive and defensive purposes while in, or expecting, contact with the enemy . . . includes assuring the mobility of friendly forces."[2]

Maneuver involves more than moving from point A to point B. Commanders must account for the enemy's position and seek a positional advantage. Gaining and maintaining EMS superiority, even if momentarily, is not only a critical objective in its own right but also a prerequisite for achieving superiority in other domains. Without EMS superiority as a foundation, military objectives against a capable EMSO adversary such as Russia will be difficult to achieve.

EMS maneuver encompasses both offensive and defensive operations. This section focuses on defensive operations, such as electromagnetic protection (EP) and defensive electronic attack (DEA).

EP and DEA

Defensive EMSOs protect personnel and equipment from physical attack and defend friendly EMS systems against enemy offensive EMSO.[3] EP may be active or passive and shields personnel and systems from enemy electronic attack (EA). Examples of EP include of EP include emissions control (EMCON), frequency agility, wartime reserve modes, anti-spoofing and anti-jamming measures, and variable pulse repetition frequencies. Defensive EA includes employing chaff, flares, towed decoys, and infrared (IR) countermeasures.

The previous section examined how Russia employs EW on the battlefield. Given those tactics and capabilities, NATO must take a holistic approach to employing EP and DEA. Commanders should synchronize these capabilities across time, space, and operational functions to counter Russian EW systems effectively.

NATO must practice EMCON during C2 activities, equip air and ground systems with appropriate defensive countermeasures, and ensure munitions incorporate anti-jam and anti-spoof technologies. Optimal combinations of EP and defensive EA should support pulsed operations designed to achieve localized EMS superiority in time and space while contributing to overall EMS superiority.

Key Components of EMS Superiority

EMS superiority is essential to the effective C2ISR, as well as the survivability of forces within a highly contested EMS environment. Three components are central to achieving EMS superiority: spectrum management, EMCON, and signals intelligence (SIGINT). Together, these functions enhance operational effectiveness and survivability against sophisticated electronic threats, including advanced Russian EW capabilities.

Joint Publication (JP) 3-85, Joint Electromagnetic Spectrum Operations, defines *spectrum management* as a continuous process that optimizes use of the EMS through operational, engineering, and administrative procedures.[4] It is not simply a matter of managing the spectrum but of ensuring its efficient use. Spectrum management encompasses the operational, engineering, and administrative procedures necessary for planning and coordinating activities within the electromagnetic operational environment.[5]

This proactive approach enables the concurrent operation of multiple users, facilitating reliable communications and the effective operation of electronic systems such as radars, navigation aids, and communications equipment in a highly contested EMS environment.

EMCON involves more than controlling emissions; it also seeks to maximize command-and-control capabilities while minimizing operational security risks. These risks include detection by enemy sensors, mutual interference among friendly systems, and adversary interference that could undermine military deception plans.[6] Therefore, EMCON serves as a precautionary tactical measure designed to reduce the EMS signature of friendly assets, thereby complicating enemy targeting and intelligence-gathering efforts. EMCON plays a critical role in maintaining surprise and protecting friendly forces from detection.

Finally, SIGINT provides valuable insights into adversary intentions, capabilities, and movements. It encompasses a broad range of intelligence, including communications intelligence (COMINT), electronic intelligence (ELINT), and foreign instrumentation signals intelligence (FISINT), regardless of transmission method.[7] By leveraging the EMS as a rich source of information, SIGINT can provide a decisive strategic and tactical advantage, making it an indispensable component of combat operations. The next section examines NATO's critical capabilities and their contribution to military operations before discussing Russian EW capabilities and their potential effects on NATO military campaign planning.

NATO Critical Capabilities

With 32 nations contributing a wide variety of military equipment, NATO operates numerous platforms that must incorporate EP and DEA while maintaining interoperability during military operations. These systems and platforms provide the critical capabilities that enable NATO to project power and conduct a successful campaign in a highly contested EMS environment.

Among the capabilities that must endure in such a scenario are satellite uplinks, downlinks, and their associated frequency bands. These links and bands carry voice and data transmissions across the force. Equally important are communications systems, including the High Frequency Global Communications System and satellite communications. These systems support battlefield deconfliction, order dissemination, and the voice and data networks NATO forces use to shoot, move, and communicate.

Another critical capability is the Global Positioning System (GPS) and NATO's suite of precision-guided munitions (PGM). GPS provides positioning, navigation, and timing (PNT), which in turn enables the effective employment of PGMs. Precision-guided munitions are particularly important for striking enemy targets while minimizing collateral damage, especially in densely populated urban environments.

Another critical capability is the anti-access/area-denial (A2/AD) architecture. Radars that support surface-to-air missile (SAM), air-defense, and air-attack systems enable integrated capabilities such as Patriot, NASAMS, and CAMM.

The final critical capability discussed is the array of airborne platforms that rely on communications systems, satellite links, GPS, PGMs, and A2/AD networks to provide ISR; battlespace awareness; artificial intelligence (AI)-enabled capabilities; defensive counterair (DCA); close air support (CAS); and unmanned aerial vehicle (UAV) operations.

A highly contested electromagnetic spectrum environment (HCEMSE) threatens the availability of these capabilities and the advantages they provide to the warfighter. Given Russia's purpose-built EW architecture, no major campaign against Russia can currently succeed without them. The next section examines the development of Russian EW capabilities and assesses their successes and failures on the battlefield.

How the Russians Fight

By 2001, the Russian Federation recognized that it could not match US military capabilities directly and shifted its focus to asymmetric investments in EW. Russian Putin, deeply affected by the collapse of the Soviet Union, perceives both a populist uprising within Russia and its near abroad and an expanding NATO alliance as direct threats to his regime. The color revolutions in Ukraine, Georgia, and Moldova between 2003 and 2005 reinforced his view that civil unrest posed one of the greatest threats to regime stability.

Russia's 2008 war with Georgia exposed several shortcomings in its EW capabilities. Its underwhelming performance prompted organizational reforms and procurement changes focused on asymmetric warfare. The 2011 Arab Spring, which toppled the governments of Libya and Egypt, further reinforced Russia's perceived need to transform its capabilities and expand its reflexive-control mechanisms.

Over time, Russian planners concluded that merely controlling or denying access to the EMS for military purposes was insufficient. As a result, the Russian conception of EW expanded to include information warfare, cyberwarfare, and network-centric warfare.[8] The Swedish Ministry of Defense observed that most Russian EW doctrinal documents have been revised since 2010 and noted that "The targets of EW are thus not limited to equipment and systems directly active in the EMS, such as radio communications equipment, radar, electro-optical sensors, and so on. Underlying systems such as computers, data storage, and energy supply systems also constitute viable targets for EW measures."[9]

The end state of Russian investment in EW is to enable information warfare capable of influencing populations, degrading foreign military effectiveness, and shaping government decision-making through cyber and electronic means.

Russian Most Likely Usage of EW in a Baltics Scenario

The most likely scenario for a Russian invasion of NATO territory would resemble Russia's campaign in Ukraine but with more disciplined employment of EW following the shortcomings revealed in 2022. Russian military strategy seeks to "impose contact on an adversary who is inclined to avoid it."[10]

Before ground forces make contact, Russian doctrine emphasizes the use of EW and network-centric warfare to disrupt enemy C4ISR and deny adversaries access to radars, communications, and electronic systems across as many frequencies as possible.[11] Russian forces employ EW to disrupt standoff precision attacks, degrade adversary information systems, and increase the survivability of troops and air defense systems.

Russian planners believe this approach will provide ground forces sufficient time to make contact with the enemy, seize key terrain in the Suwałki Gap, and establish defensive positions. If NATO can demonstrate that it has retained its C2 and strike capabilities before ground forces engage, it may deter or delay a Russian invasion.

Should NATO assess that Russian forces are preparing an offensive against the Baltic states, it must be prepared to counter Russian EW aggressively during the noncontact phase to prevent the invasion from gaining momentum.

Russian EW Usage and Lessons from Ukraine/Syria

Since Russia shifted toward a heavy emphasis on electronic warfare (EW), intelligence agencies have been able to observe how these capabilities integrate into a combined-arms maneuver force. Russia employed these capabilities in Crimea and the Donbas from 2014 to 2021, in Syria from 2015 to 2018, and during its full-scale invasion of Ukraine beginning in 2022.

In the opening stages of Russia's campaign in the Donbas in 2014, Russian forces reportedly employed a virus or kill switch embedded in radios previously supplied to Ukraine. The resulting communications degradation forced Ukrainian forces to rely on commercial cellular phones and high-frequency (HF) radio. Russia then jammed radio communications in the 137–180 MHz and 400–470 MHz bands and successfully exploited soldiers' smartphones to identify Ukrainian unit positions on the battlefield.[12]

Russia also employed disinformation and psychological operations against soldiers and civilians through its Leer-3/Orlan-10 EW system. This system exploited personal information from smartphones and sent mass text messages intended to threaten soldiers' families and deceive Ukrainian commanders with false orders at distances of up to 20 kilometers.[13] These communication-denial and information-deception tactics proved highly effective in the near battlespace.

Between 2015 and 2018, Russia redeployed several EW brigades from Ukraine to support the Syrian government. In Syria, these units employed counterspace EW capabilities to deny and spoof GPS signals with effects reportedly reaching as far as Tel Aviv, Israel, disrupting airport operations.[14] US and UK commanders also acknowledged that Russian EW units deliberately jammed NATO aircraft systems operating over Syria and Jordan.[15] These activities likely allowed Russia to test and refine its ability to deny GPS-guided munitions, disrupt US aircraft communications, and degrade space-based intelligence collection.

After years of employing EW in Ukraine and Syria, many observers expected Russia's 2022 invasion of Ukraine to benefit significantly from those capabilities. Surprisingly, Russian EW proved largely ineffective in supporting combined-arms maneuver and produced only limited effects against Ukrainian forces. Three major lessons emerge from the conflict.

First, Ukrainian forces adapted to a degraded EMS environment during eight years of fighting in Crimea and the Donbas. They improved emissions-control discipline and delegated decision-making authority to small-unit maneuver elements, allowing them to “shoot and scoot” before Russian counterattacks could target their positions. The influx of NATO equipment after 2022 also provided more secure communications, reducing the effectiveness of Russian jamming and restoring operational-level command and control.

Second, Ukraine demonstrated a substantial ability to disrupt Russian command and control by employing similar tactics and technologies. Ukrainian forces exploited Russian emissions through signals intelligence (SIGINT), taking advantage of poor Russian EMCON practices. They also employed offensive electronic attacks against Russian units that lacked adequate electronic protection. Successful jamming forced Russian troops onto cellular and other unsecured communication systems, mirroring tactics Russia had previously used against Ukraine. Ukrainian forces then used electronic direction-finding techniques to conduct rapid counterbattery fires against Russian positions.

Finally, neither side was able to suppress enemy air defenses sufficiently to establish air superiority, resulting in a World War I–style artillery duel along a largely static front. One contributing factor has been the ability of EW systems to interfere with munition terminal guidance, causing precision weapons to miss their targets. Additional EW measures, including decoys, false emitters, and frequency-agile radar systems, have further complicated efforts to employ airborne assets in support of ground offensives. The high cost and risk associated with losing advanced fighter and bomber aircraft to EW-protected air defenses have made attempts to establish air superiority increasingly impractical. As a result, a decisive breakthrough by either side appears unlikely without the development of more effective counter-EW capabilities.

Russian EW Force Organization

The Russian Armed Forces have embraced EW and organized EW brigades (REB) throughout the joint force. The Russian Ground Forces appear to be the leading proponent of EW capabilities and have fielded some of Russia’s most capable EW systems. Between 2009 and 2016, Russia formed five EW brigades to support its military districts and established an additional EW headquarters brigade in Tambov. Each naval fleet (Baltic, Black Sea, Northern, and Pacific) also created an EW brigade under fleet command. At the same time, the Aerospace Forces established five air-defense EW battalions to support integrated air and missile defense operations.

Regardless of the service they support, EW units are primarily ground based and operate from wheeled or tracked vehicles. Each EW brigade fields higher-level systems such as the Krasukha-2, Krasukha-4, Leer-3, and Murmansk-BN.[16] These brigades typically consist of four to five subordinate battalions organized according to the types of systems they are designed to counter. The principal categories are:[17]

- **REB-N**—EW against ground-based systems
- **REB-S**—EW against airborne systems
- **REB-K**—EW against space-based systems
- **REB-Atd**—EW against terrorist activities
- **KTK**—Comprehensive technical control (electronic support)

The Russian General Staff places significant emphasis on these EW brigades and will likely rely on them to deter and degrade enemy forces during the opening stages of a conflict. In 2018, Major General Yuriy Lastochkin, commander of Russia's REB force, stated that REB's men and equipment will permit Russia "to decide the fate of all military operations."[18]

The following EW units are the most likely to participate in a conflict with NATO in the Baltic region:

15th EW Brigade Headquarters (Tambov, Russia). This brigade serves as the EW schoolhouse and headquarters for Russia's EW commander. It functions as a "mobile brigade," allowing it to deploy to any military district with subordinate REB-N, REB-S, and REB-K battalions.[19] The brigade likely controls some of Russia's most capable theater-level EW systems and should therefore be considered a high-priority target.

16th EW Brigade (Kursk, Russia). This brigade supports ground-force protection against artillery, unmanned aerial vehicles (UAVs), and precision-guided munitions. It also fields multiple communications-jamming and information operations (IO) systems and includes theater-level capabilities designed to affect NATO C4ISR.

841st EW Center (Yantarny, Kaliningrad). Reporting directly to the Baltic Fleet commander, this unit provides EW support and protection for Kaliningrad. It consists of two battalions. One battalion conducts "strategic EW tasks," including SIGINT and ELINT collection and the employment of electronic decoys to protect strategic systems.[20] The second is the 328th EW Battalion, which supports the Kaliningrad integrated air defense system (IADS).

328th EW Battalion (Pesochnye, Kaliningrad). This REB-S unit supports the 6th Air and Air Defense Army in the Western Military District. It contributes to the protection of the Kaliningrad IADS and A2/AD systems intended to restrict NATO air operations over the battlespace.

Russian EW Equipment Capability

A 2020 MITRE report on Russian EW trends stated, "Russia has more than 30 different REB systems in the ground forces alone to attack unmanned aerial vehicles (UAVs), radars, GPS frequencies, cellular networks, and other command-and-control or communications devices."[21] The report further suggests that REB units are attempting to create an "electronic dome" over the battlefield by exploiting perceived US and NATO reliance on EMS access for space-based C4ISR, positioning, navigation, and timing (PNT), and weapon guidance.

This effect is achieved through the combined use of three systems: a Borisoglebsk SIGINT collection capability, a Krasukha system capable of suppressing aircraft radar emissions and drone control links, and a Zhitel system that can jam satellite communications, navigation equipment, and cellular communications within a radius of 30 kilometers.[22]

The following systems and capabilities are identified in unclassified open-source reporting. Inclusion in this discussion does not validate specific performance claims or imply the existence of classified capabilities. The systems described below are drawn primarily from the 2020 MITRE report *Russia's Electronic Warfare Force* and the 2018 Swedish Defence Research Agency report *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces*:

- **RB-109A Bylina EW Command-and-Control System**: This system independently identifies and selects targets—including radio stations, communications systems, radars, airborne early-warning aircraft, satellites, and other facilities—within seconds. It employs AI to determine suppression methods and select the most effective jamming systems.[23]
- **Borisoglebsk-2**: The latest Russian iteration of the Soviet R-330 Mandat complex. The system consists of several EW components mounted on nine MT-LB tracked vehicles that collectively provide tactical SIGINT, communications jamming, and the ability to target radio, satellite communications, and navigation systems.[24]
- **Rtut-BM**: This system creates a protective "dome" over a defended site, causing munitions to detonate at a safe distance.[25] It counters enemy weapons equipped with radio-controlled detonators by neutralizing proximity-fuse systems.[26]

- **Palantin**: Designed to suppress operational- and tactical-level communications systems based on software-defined radio (SDR) technology. The system reportedly possesses a "system-forming" capability that allows it to integrate multiple jamming systems and improve their collective effectiveness.[27]
- **Leer-2**: This system conducts ELINT collection and jams electronic equipment.[28]
- **Leer-3**: Consisting of three Orlan-10 UAVs, this system can jam 3G and 4G cellular communications, conduct reconnaissance, and transmit targeting data to artillery units. It can also send mass audio, text, and video messages to cellular phones.[29]
- **R-330 Zhitel**: This automated jamming station targets UAVs at ranges exceeding 20 kilometers. It can disrupt cruise-missile and precision-weapon guidance systems. Zhitel can also detect, locate, and jam satellite and cellular communications networks, as well as satellite navigation systems, including GPS, within a radius of 20–30 kilometers.[30]
- **Murmansk-BN**: Capable of jamming military communications networks at ranges of up to 5,000 kilometers—and under some conditions up to 8,000 kilometers—this shore-based system can collect ELINT and intercept or jam signals across the shortwave spectrum.[31]
- **Moskva-1**: This command-and-control system includes ELINT capabilities and can integrate up to nine Krasukha-family jamming systems operating at different locations. It can also provide target data to air-defense C2 systems and reportedly triangulate the location of emitting aircraft or cruise missiles at distances of up to 400 kilometers.[32]
- **Krasukha-2**: This system detects and jams ground-based and airborne radars. It can disrupt aircraft systems at ranges of up to 300 kilometers and interfere with C2 links for UAVs and cruise missiles.[33]
- **Krasukha-4**: Designed to counter aircraft radars, communications, and data-transfer systems, this system can jam a wide range of radar emitters. It can also degrade UAVs, reconnaissance aircraft, and low-Earth-orbit satellites.[34] Its estimated range is 150–300 kilometers.[35]
- **Sapsan**: This system has an operating radius of approximately 100 kilometers. Its search capabilities include radar, visible-spectrum and IR sensors, and electronic reconnaissance. It can direct electromagnetic jamming against drone swarms approaching from a single axis.[36]

- **Khibiny**: Installed on the Su-34 and compatible with several Flanker variants, including the Su-30 and Su-57, this system can create false radar returns and generate a deceptive electronic picture.[37]
- **Pole-21**: This system employs suppression and jamming modules designed to counter drones and reduce the effectiveness of cruise missiles. It can also suppress signals from multiple satellite navigation systems, including GPS, Galileo, and BeiDou. [38]

Russian Ground Forces

Russian ground forces rely on centralized command and control to maneuver against an adversary. This top-down approach originates from the Soviet Union and does not encourage initiative or decentralized execution below the battalion tactical group (BTG) level. The principal decision-makers who link tactical actions to operational objectives reside above the BTG echelon.

Russia historically used a brigade-based model to generate BTGs. Individual brigades formed BTGs that operated under a Combined Arms Army (CAA), which maneuvered the BTGs and managed many aspects of the deep and close fight to facilitate ground operations. Based on its experiences in Ukraine, however, Russia is shifting from a brigade-generated BTG model under a CAA to a division-based structure with multiple regiments capable of organizing and commanding BTGs. This structure allows Russia to employ BTGs composed of contract soldiers while army, division, and brigade formations generate replacement BTGs from conscripts. Army and division headquarters retain command of employed BTGs and allocate additional forces according to operational requirements. Mission requirements for BTGs are determined at the CAA or division echelon. These higher headquarters synchronize warfighting functions across subordinate BTGs and coordinate strikes to facilitate maneuver.

This organizational change adds an additional command-and-control layer between the CAA and the BTG. The division echelon synchronizes multidomain effects on the battlefield and directs BTG maneuvers. Russian strike operations, coordinated at the division and CAA levels, support BTGs through massed fires designed to create favorable conditions for maneuver.

The BTG is the smallest Russian ground-force formation capable of conducting all warfighting functions while maneuvering. Small-unit leaders below the BTG level are not generally empowered to make independent decisions and are expected to adhere closely to the unit's operational plan. Russian commanders favor this approach because centralized control compensates for the uneven proficiency of conscript personnel. Units below the BTG rely on preplanned actions to conduct tactical engagements, giving commanders at the BTG level and above a greater sense of control. As one observer notes, centralized control takes precedence over small-unit initiative to prevent independent actions that might "undermine a commander's overall plan."[39]

Russian ground forces seek to employ fires, or strikes, at the time and place that will best "facilitate ground success."[40] The Russian military defines a *strike* as "the convergence of multiple effects, to include multiple domains, focused on an aggressor force."[41] Russian headquarters integrate reconnaissance, intelligence collection, and targeting through networked command-and-control systems to employ strikes effectively against an adversary.[42]

At the strategic and operational levels, strikes constitute the primary means of achieving military objectives, while tactical fires serve as supporting or culminating actions.[43] Russian BTGs and subordinate units integrate organic fires with higher-echelon assets and adjacent formations to mass effects against an adversary.[44] The CAA controls strike assets allocated in support of ground maneuver forces, assigning them to division and brigade echelons as required.[45] Divisions and brigades plan and coordinate these strikes, which are then executed to maximize destructive effects and facilitate mission accomplishment. Because planning is highly centralized, firing units typically engage preplanned targets during execution to shorten the kill chain. Fire direction centers coordinate these engagements and "pass all detected high-value targets directly to firing units without headquarters analysis and direction."[46]

CAAs also form task-organized reconnaissance-strike complex (RSC) units to engage high-value targets. As one analyst observes, "The old stereotype of the Soviet and Russian military being an artillery army with maneuver units attached remains largely true."[47]

Desired System

The desired system encapsulates the outcomes NATO seeks to achieve in a conflict involving advanced Russian EW capabilities. It reflects the strategic objectives necessary to ensure superiority within the EMS. Key criteria include the following:

1. **EMS Access and Control**: Ensure persistent and unimpeded access to the EMS, enabling NATO forces to maintain C2 across all joint operational areas.
2. **Resilience to EW Threats**: Develop robust EP measures and countermeasures that mitigate Russian EW capabilities and preserve NATO operational effectiveness against EA.

3. **Integrated EMS Operations**: Establish an integrated approach to EMS operations that synchronizes ISR, personnel, and kinetic and nonkinetic capabilities across NATO forces to exploit Russian vulnerabilities and effectively counter Russian operational strategies.
4. **Adaptive and Flexible Response Capabilities**: Create an operational environment in which NATO forces can rapidly adapt to evolving EW tactics, techniques, and procedures (TTP) and exploit near-real-time intelligence to disrupt Russian operations.
5. **Long-Term EMS Superiority**: Cultivate foundational training, capabilities, and rapidly evolving TTPs that address immediate threats while positioning NATO and its allies to maintain long-term EMS superiority.

Desired End State: NATO maintains continuous access to the EMS throughout a conflict with Russia, enabling effective command and control, countering enemy EW and A2/AD systems, and safeguarding allied territory by repelling Russian aggression.

Problem Sets

The following problem sets identify the challenges NATO must overcome to transition from the current observed system, characterized by vulnerabilities to Russian EW capabilities, to the desired system.

1. **Countering Russian A2/AD and EW Systems**: NATO must address the technological and strategic challenges posed by integrated Russian A2/AD and advanced EW capabilities that threaten to degrade NATO's ability to respond effectively.
2. **Integrating Cross-Domain EW Operations**: NATO must develop mechanisms to better integrate EW TTPs across all military domains to enhance operational effectiveness.
3. **Technological and TTP Adaptation**: NATO must continue investing in new technologies and TTPs to maintain an advantage over evolving Russian EW capabilities, including the development of artificial intelligence and machine learning (AI/ML) solutions for EMS operations, integration, and training.
4. **Alliance Cohesion and Response Speed**: NATO must maintain a cohesive and rapid response to EW threats by streamlining C2ISR structures and improving interoperability through training and exercises.

5. **Training and Doctrine Development**: Developing training programs at the foundational level is essential to keeping pace with rapidly evolving military TTPs. Incorporating advanced EMS and EW concepts into core training will better prepare NATO forces for operations in HCEMSEs.
6. **Resource Allocation and Strategic Prioritization**: NATO must prioritize resources for the development and deployment of systems capable of countering Russian EW capabilities while ensuring investments align with strategic requirements.

Problem Statement: Russia has demonstrated a high degree of proficiency in employing electronic warfare, and its operational approach depends on effective control of the electromagnetic spectrum. In the event of a Russian invasion of the Baltics, how can the United States and NATO gain and maintain a positional advantage in the EMS to halt the attack?

Operational Approach

The operational approach describes how NATO can transition from the observed system to the desired system by addressing the identified problem sets and achieving the desired end state. Because access to and maneuver within the EMS underpin modern military operations, NATO must prioritize actions that protect its own EMS-dependent capabilities while degrading those of its adversary. The following lines of effort provide a framework for achieving EMS superiority and creating the conditions necessary for successful JADOs against Russian forces.

Lines of Effort Overview

Three lines of effort are recommended to gain a positional advantage in the EMS. These lines of effort are (1) developing NATO EP measures and maneuverability within the EMS, (2) employing offensive EW against Russian forces to disrupt an advance, and (3) identifying and countering Russian EW capabilities. US and NATO forces rely on access to the EMS to enable military operations. Because modern military forces are fundamentally dependent on EMS-enabled capabilities, NATO's priorities in the period leading to a conflict should focus on degrading Russian offensive EW capabilities while improving the protection and maneuverability of allied forces within the EMS. Together, these lines of effort provide a framework that joint force planners can incorporate into operational plans.

Objectives

1. Defend Baltic territorial integrity by defeating or repelling Russian aggression.
2. Enable freedom of maneuver in the air domain by targeting A2/AD systems protected by EW capabilities.
3. Enable NATO C4ISR and space-based capabilities by maintaining access to the EMS.

LOE 1: NATO Electronic Protection Measures and Maneuverability in EMS

Planning

NATO must also consider EP for stationary nodes, command centers, war-supporting facilities, and tactical-unit communications to protect the link from sensor to shooter. Defensive cyber operations, as part of the EMS environment, should be updated and integrated to counter Russian offensive cyber capabilities.

How should NATO adapt EP and DEA planning to address modern Russian EW capabilities? Key considerations include operational preparation of the environment, a threat-specific focus, and the use of nontechnical means when advantageous. NATO planners must first develop a comprehensive understanding of the operational environment (see the preceding discussion of Russian EW). Questions include the location of Russian EW systems, their effective ranges, the relationships among system components, the EP and DEA measures Russia employs, and the extent to which Russian systems are vulnerable to jamming, spoofing, and other forms of military deception. Such questions help planners develop a more complete understanding of the operational environment and the challenges posed by Russian EW.

With support from the intelligence community, planners can then identify which NATO systems are best suited to counter specific Russian EW capabilities. They should match NATO strengths against Russian vulnerabilities and identify capability gaps requiring mitigation. Where possible, NATO should modify platforms and tactics to address these gaps or employ nontechnical solutions. Such solutions may include special operations forces, sabotage, and other human-focused approaches to find, fix, track, and destroy high-value EW targets that are difficult to attack through kinetic or air-delivered means.

Once planners understand NATO and Russian EW strengths and vulnerabilities, they can organize forces to enter and operate within a high-threat EW environment in a manner that maximizes survivability and increases the likelihood of mission success.

Strategic Value Through Spectrum Superiority

Russia is a formidable adversary that relies on asymmetric methods and tactics to disrupt its opponents through the effective employment of EW. While Western forces often focus on the broader A2/AD challenge, Russia continues to develop capabilities designed to degrade Western C2. These developments underscore the importance of spectrum management, EMCON, and SIGINT.[48]

At the same time, Russian operations are often hindered by shortcomings in synchronization and integration. Understanding the relationship among spectrum management, EMCON, and SIGINT helps illuminate their strategic value in a HCEMSE. These functions are more than operational tools; when integrated effectively, they can provide a significant asymmetric advantage. This section examines contemporary challenges to C2ISR in an HCEMSE and explains how EMS superiority can create operational advantages against sophisticated EW adversaries such as Russia.

Lessons from the Russo-Ukrainian War reinforce the need to integrate EMS concepts and doctrine into foundational education and training, consistent with the Department of War's EMS superiority strategy. This includes concepts such as electromagnetic battle management, which leverages trusted data sources, including SIGINT, to improve spectrum awareness through human-supervised machine-to-machine collaboration.[49]

Friendly forces must also accelerate EMS integration into operational planning and capitalize on commercial technologies such as AI/ML. AI-enabled systems are already demonstrating combat effectiveness in unmanned platforms that use autonomous object recognition. Although these capabilities are available on expensive American-made systems, Ukraine has demonstrated that comparatively inexpensive drones employing less sophisticated algorithms can successfully attack Russian air-defense systems.[50]

NATO should therefore invest substantially in AI/ML applications that can mitigate jamming effects and improve target recognition for long-range fires. One theoretical application would combine AI/ML-enabled digital radio-frequency memory with software-defined-radio signals transmitted through a phased-array conformal antenna mounted on a low-cost drone, potentially increasing survivability in contested environments. Investments in training, operational planning, and AI/ML integration may ultimately provide a decisive advantage to militaries willing to adopt and refine these technologies.

Achieving EMS superiority against advanced adversaries such as Russia requires the integration of spectrum management, EMCON, and SIGINT into military strategy and operations. The dynamic nature of EW rewards organizations that combine technological innovation with tactical adaptation. Robust training, deliberate integration into operational planning and deconfliction processes, adaptive tactics, and investments in emerging technologies such as AI/ML can serve as both immediate force multipliers and long-term strategic advantages. Success in future conflicts will depend on the ability to innovate, adapt, and effectively integrate these capabilities, thereby enhancing operational effectiveness, improving survivability, and preserving a decisive advantage in the EMS.

LOE 2: EW Usage to Degrade Russian Ground Forces

A future conflict between NATO and Russia will likely favor the side that can disrupt its opponent's ground operations. Degrading Russia's centralized control of ground maneuver through EA would significantly undermine its offensive capabilities. Isolating Russian ground forces at the battalion tactical group (BTG) level from division and CAA headquarters would severely impair their ability to maneuver effectively. Russian units at the BTG level and below are often slow to adapt to rapidly changing battlefield conditions because they rely heavily on guidance from higher headquarters. This dependence on centralized control creates a vulnerability that NATO can exploit.

Russian C2 networks and RSCs therefore present high-payoff targets for EA. Disrupting communications between BTGs and their higher headquarters would degrade the Russian military's ability to synchronize operations and execute offensive maneuvers. The Russian Army places a premium on centralized control and discourages initiative at lower levels. As a result, the headquarters that link tactical actions to operational objectives—particularly division headquarters—play a critical role in enabling ground operations and coordinating strikes.

Severing the communication link between BTGs and division headquarters would leave many Russian units unable to respond effectively to changing battlefield conditions. Simultaneously disrupting the RSC's ability to sense, identify, and support targets would further degrade Russian combat effectiveness. Divisions unable to coordinate with subordinate BTGs would struggle to employ RSCs effectively, undermining their ability to support maneuver operations.

Targeting these C2 relationships and reconnaissance-strike capabilities would exploit a fundamental weakness in the Russian approach to warfare. By disrupting the links between higher headquarters and subordinate maneuver units, NATO could significantly reduce Russia's ability to coordinate fires, maneuver forces, and sustain offensive momentum.

LOE 3: Identifying and Countering Russian Offensive EW

To effectively counter a system of systems such as Russian offensive EW, NATO must find, fix, track, and engage critical nodes to degrade the capability and deny its effectiveness on the battlefield. This line of effort seeks to fill critical intelligence gaps by locating EW assets and targeting EW brigade operators and theater-level EW systems. Preventing these systems from transmitting and jamming radio-frequency bands would help ensure NATO access to the EMS.

Intelligence Collection

Intelligence collection efforts should prioritize determining the locations of Russian EW brigades and identifying which EW systems are being prepared for employment. Of the dozen or so EW brigades established across the Russian military, four are the most likely to be employed in a Baltic conflict scenario. Intelligence planners should prioritize identifying and tracking the following units before a crisis or conflict begins:

- 15th EW Brigade Headquarters (Tambov, Russia; EW schoolhouse and headquarters for the EW commander)
- 16th EW Brigade (Western Military District, Kursk, Russia)
- 841st EW Center (Baltic Fleet unit, Yantarny, Kaliningrad, Russia)
- 328th EW Battalion (Pesochnye, Kaliningrad, Russia)

Each EW brigade headquarters typically controls approximately six theater-level EW systems with the greatest potential to influence battlefield operations. These systems are generally larger, have limited off-road mobility, and tend to operate near brigade headquarters locations. Intelligence planners should employ all available SIGINT, ELINT, and human intelligence capabilities to find, fix, and track these systems. Locating and monitoring EW brigade headquarters should be included among a joint force commander's priority intelligence requirements.

The following theater-level systems are likely to operate near EW brigade headquarters and should be included on the joint integrated prioritized target list at the outset of a conflict:[51]

- RB-109A Bylina
- Murmansk-BN
- RB-341V Leer-3
- IRL-257 Krasukha-4
- IL-269 Krasukha-2
- IL-267 Moskva-1

Methodology to Engage Russian EW Systems

Several methods can reduce or negate the effects of Russian EW systems. The most effective approach is to prevent the transmitter from operating. This can be accomplished through physical destruction, electronic disruption, denial of operational access, supply-chain interdiction, or psychological operations directed at system operators.

Physical Destruction: Destroying transmitters through kinetic means, such as bombs or anti-radiation missiles, would likely produce the most enduring effects, although it may also be the most difficult option to execute.

Electronic Damage: Directed-energy weapons or electromagnetic pulse–like effects could damage sensitive electronic components and render systems inoperable. Temporary effects may be sufficient to support planned pulsed operations.

Proximity: Most tactical EW systems have effective ranges of less than 20 kilometers. Because these systems are typically mounted on large trucks or trailers, mobility can be constrained by terrain and fuel availability. Rough terrain or disruptions to fuel supplies may prevent systems from reaching locations where they can operate effectively.

EW Manufacturers and Supply Lines: Russian EW systems rely on advanced semiconductor microchips, many of which Russia cannot produce domestically. As a result, it depends on components sourced from abroad, including from China and through third-party intermediaries. Although the United States, Taiwan, and the European Union have imposed restrictions on technology exports, reexports through third countries continue to provide Russia with access to critical components. Closing these loopholes could provide a long-term means of limiting Russia's EW production capacity. Actions directed against manufacturers and supply chains may also generate intelligence regarding system capabilities and production vulnerabilities.

Major organizations associated with the development and production of Russian EW systems include:[52]

- **CRET**: Bylina manufacturing
- **Kvant**: Krasukha-2/4, Moskva-1 research and development
- **Gradient**: Rtut-BM research and development
- **Revtrud**: Rtut-BM and Borisoglebsk-2 manufacturing
- **TNIIR**: Borisoglebsk-2 research and development
- **BEMZ**: Krasukha-2/4 manufacturing
- **STTs**: Leer-3 manufacturing
- **KNIRTI**: Khibiny and Tarantul manufacturing

Psychological Operations (PSYOP): Influencing the behavior of EW operators can be as effective as destroying equipment. If operators believe activating a system significantly increases their risk of being targeted, they may become reluctant to employ it. Similar effects were observed during the Gulf War, when Iraqi surface-to-air missile operators often hesitated to activate radar systems because of the threat posed by anti-radiation missiles. US forces reportedly reinforced this hesitation by exploiting Iraqi perceptions of risk. A comparable approach could be employed against Russian EW operators to discourage system use and reduce operational effectiveness.

Conclusion

Advanced Russian EW capabilities present a significant challenge to NATO's operational effectiveness and its ability to preserve territorial integrity in the face of aggression. The central challenge confronting NATO is securing and maintaining a positional advantage in the EMS during a conflict with Russia. This study underscores the importance of the EMS as a foundational domain that enables military operations across all other domains.

The analysis highlights the strategic importance of spectrum management, EMCON, and SIGINT as key pillars of EMS superiority. These capabilities are not merely operational tools but strategic assets that, when effectively integrated, can provide an asymmetric advantage in warfare. Given Russia's demonstrated proficiency in EW, NATO and its allies must adopt adaptive and evolving countermeasures to preserve freedom of action in the EMS.

Key Recommendations

1. **Enhance EMS and EW Discipline and Training**: Expand foundational EMS training and conduct additional joint and coalition exercises to improve operational readiness, spectrum awareness, spectrum management, and EMCON discipline.
2. **Develop Advanced EA/EP Capabilities**: Invest in advanced technologies, including AI/ML-enabled SDRs, to counter and neutralize adversary EW threats.
3. **Pursue Coordinated Offensive EA**: Prioritize Russian division headquarters and other key EW assets to degrade C2 capabilities and disrupt offensive operations through offensive electronic attack.
4. **Deny, Degrade, and Destroy Russian the Four Priority Russian EW Brigades**: Focus intelligence, targeting, and operational efforts on identifying, exploiting, and neutralizing the four priority Russian EW brigades to reduce their ability to support Russian military operations.
5. **Invest in Long-Term EMS Superiority**: Commit sustained resources to the development and refinement of defensive and offensive technologies and TTPs necessary to maintain NATO's long-term advantage in the EMS.

EMS superiority remains a decisive factor in modern warfare. It underpins effective C4ISR capabilities and contributes directly to the security and defense of NATO member states. By addressing the challenges outlined in this study through a coordinated and innovative approach, NATO can establish and maintain a lasting asymmetric advantage in the EMS.

Notes

1. Joint Publication 3-85, *Joint Electromagnetic Spectrum Operations* (Government Publishing Office, May 22, 2020), I-6.

2. Joint Publication 3-0, *Joint Operations* (Government Publishing Office, June 18, 2022).

3. Joint Publication 3-85, I-5.

4. Ibid.

5. Ibid.

6. Ibid.

7. Ibid.

8. Jonas Kjellén, *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces* (Swedish Defence Research Agency [FOI], April 10, 2018), 13, https://www.foi.se/.

9. Ibid., 21.

10. Clint Reach, Alexis A. Blanc, and Edward Geist, *Russian Military Strategy: Organizing Operations for the Initial Period of War* (Santa Monica, CA: RAND Corporation, 2022), 74, https://www.rand.org/.

11. Ibid., 77.

12. Joseph Trevithick, "Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio Virus," *War Zone*, October 30, 2019, https://www.twz.com/.

13. Arie Egozi, "Why Would Russia Spoof Israeli GPS? F-35 & Iran," *Breaking Defense*, July 22, 2021, https://breakingdefense.com/.

14. Ibid.

15. Ibid.

16. Bryan Clark, "The Fall and Rise of Russian Electronic Warfare," *IEEE Spectrum*, November 22, 2022, https://spectrum.ieee.org/.

17. Kjellèn, *Russian Electronic Warfare,* 36.

18. Aleksandr Stepanov interview with Yuriy Illarionovich Lastochkin, "They Have Deployed a Dome Which Defends from Missiles Over the Russian Bases in Syria," *MK Online*, 15 April 2018. Cited in Timothy Thomas, *Advanced Weaponry and Russian Military Art of War* (MITRE, September 2020), 3, https://www.mitre.org/.

19. Kjellèn, *Russian Electronic Warfare*, 36.

20. Konrad Muzyka, *Russian Forces in the Western Military District* (CNA, June 2021), 47, https://www.cna.org/.

21. Timothy Thomas, *Russia's Electronic Warfare Force: Blending Concepts with Capabilities* (MITRE, September 2020), 6, https://www.mitre.org/.

22. "Central Military District Electronic Warfare Specialists Test New Way of Countering Enemy Airborne Assets," *Ministry of Defense of the Russian Federation*, June 10, 2019.

23. "Bylina System RB-109A," *TAdviser*, September 29, 2017.

24. Kjellèn, *Russian Electronic Warfare,* 43.

25. "EW Specialists Placed Command Post Under Protective Dome during Exercise in Kemerovskaya Oblast," *Ministry of Defense of the Russian Federation*, March 19, 2019.

26. "Central Military District Electronic Warfare Subunits in Siberia Receive Newest Rtut-BM System," *Ural'skiye Voyennyye Vesti*, May 8, 2019.

27. Kjellèn, *Russian Electronic Warfare*, 46.

28. Thomas, *Russia's Electronic Warfare Force*, 16.

29. Ibid., 16.

30. Ibid., 19.

31. "Russia Is Deploying the Murmansk-BN Electronic Warfare System to the Kaliningrad Region," *Izvestiya Online*, April 26, 2019.

32. Kjellèn, *Russian Electronic Warfare,* 52.

33. Ibid., 53.

34. Ibid.

35. Aleksey Ramm, Bogdan Stepovoy, and Aleksey Kozachenko, "Electronic Shield: Defense Ministry Deploying Electronic Warfare Resources in Syria," *Izvestiya Online*, September 25, 2018.

36. Thomas, *Russia's Electronic Warfare Force*, 18.

37. Ibid., 17.

38. Ibid., 18.

39. Philip G. Wasielewski, "The Roots of Russian Military Dysfunction," *Foreign Policy Research Institute*, March 31, 2023, https://www.fpri.org/.

40. Department of the Army, Army Techniques Publication (ATP) 7-100.1, *Russian Tactics*, 9 April 2024, 2–6.

41. Ibid., 2-10.

42. Ibid., 2-11.

43. Ibid., 5-1.

44. Ibid., 5-3.

45. Mason Clark and Karolina Hird, "Russian Regular Ground Forces Order of Battle," *Institute for the Study of War*, October 12, 2023, 13, https://www.understandingwar.org/.

46. ATP 7-100.1, 5-7.

47. Clark, "Russian Regular Ground Forces," 12–13.

48. Thomas, *Russia's Electronic Warfare Force*.

49. Mark T. Esper, *Department of Defense Electromagnetic Spectrum Superiority Strategy* (Department of Defense, October 2020), https://media.defense.gov/.

50. "How Cheap Drones Are Transforming Warfare in Ukraine," *The Economist*, February 5, 2024, https://www.economist.com/.

51. Thomas Withington, "Russian Radiation," *Armada International*, November 10, 2022, https://www.armadainternational.com/.

52. Kjellèn, *Russian Electronic Warfare,* 72.

List of Acronyms

Acronym	Definition
A2/AD	Anti-Access/Area Denial
AFDP	Air Force Doctrine Publication
AI	Artificial Intelligence
AI/ML	Artificial Intelligence/Machine Learning
BTG	Battalion Tactical Group
C2	Command and Control
C2ISR	Command and Control, Intelligence, Surveillance, and Reconnaissance
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CAA	Combined Arms Army
CAMM	Common Anti-Air Modular Missile
CAS	Close Air Support
CNA	Center for Naval Analyses
COMINT	Communications Intelligence
DCA	Defensive Counterair
DEA	Defensive Electronic Attack
EA	Electronic Attack
ELINT	Electronic Intelligence
EMCON	Emissions Control
EMS	Electromagnetic Spectrum
EMSO	Electromagnetic Spectrum Operations
EP	Electromagnetic Protection
EW	Electronic Warfare
FOI	Swedish Defence Research Agency (*Totalförsvarets forskningsinstitut*)
GPS	Global Positioning System
HCEMSE	Highly Contested Electromagnetic Spectrum Environment
HF	High Frequency
IADS	Integrated Air Defense System
IR	Infrared
ISR	Intelligence, Surveillance, and Reconnaissance
JADO	Joint All-Domain Operations
JP	Joint Publication
KTK	Comprehensive Technical Control (Electronic Support)

Acronym	Definition
NATO	North Atlantic Treaty Organization
PGM	Precision-Guided Munition
PNT	Positioning, Navigation, and Timing
RAND	RAND Corporation
REB	Radio-Electronic Warfare Brigade
RSC	Reconnaissance-Strike Complex
SAM	Surface-to-Air Missile
SDR	Software-Defined Radio
SIGINT	Signals Intelligence
TTP	Tactics, Techniques, and Procedures
UAV	Unmanned Aerial Vehicle
US	United States

Bibliography

"Central Military District Electronic Warfare Subunits in Siberia Receive Newest Rtut-BM System." *Ural'skiye Voyennyye Vesti*, May 8, 2019.

Christianson, John. "Fighting and Winning in the Electromagnetic Spectrum." *War on the Rocks*, December 5, 2022. https://warontherocks.com/.

Clark, Bryan. "The Fall and Rise of Russian Electronic Warfare." *IEEE Spectrum*, November 22, 2022. https://spectrum.ieee.org/.

Clark, Mason, and Karolina Hird. "Russian Regular Ground Forces Order of Battle." *Institute for the Study of War*, October 12, 2023. https://www.understandingwar.org/.

Department of the Army. *Army Techniques Publication (ATP) 7-100.1: Russian Tactics*. Department of the Army, April 9, 2024.

Egozi, Arie. "Why Would Russia Spoof Israeli GPS? F-35 & Iran." *Breaking Defense*, July 22, 2021. https://breakingdefense.com/.

Esper, Mark T. *Department of Defense Electromagnetic Spectrum Superiority Strategy*. Department of Defense, October 2020. https://media.defense.gov/.

"How Cheap Drones Are Transforming Warfare in Ukraine." *The Economist*, February 5, 2024. https://www.economist.com/.

Joint Chiefs of Staff. *Joint Publication 3-0: Joint Operations*. Government Publishing Office, June 18, 2022.

———. *Joint Publication 3-85: Joint Electromagnetic Spectrum Operations*. Government Publishing Office, May 22, 2020.

Kjellén, Jonas. *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces*. Stockholm: Swedish Defence Research Agency (FOI), April 10, 2018. https://www.foi.se/.

Ministry of Defense of the Russian Federation. "Central Military District Electronic Warfare Specialists Test New Way of Countering Enemy Airborne Assets." June 10, 2019.

———. "EW Specialists Placed Command Post Under Protective Dome during Exercise in Kemerovskaya Oblast." March 19, 2019.

Muzyka, Konrad. *Russian Forces in the Western Military District*. Arlington, VA: CNA, June 2021. https://www.cna.org/.

Ramm, Aleksey, Bogdan Stepovoy, and Aleksey Kozachenko. "Electronic Shield: Defense Ministry Deploying Electronic Warfare Resources in Syria." *Izvestiya Online*, September 25, 2018.

Reach, Clint, Alexis A. Blanc, and Edward Geist. *Russian Military Strategy: Organizing Operations for the Initial Period of War*. Santa Monica, CA: RAND Corporation, 2022. https://www.rand.org/.

"Russia Is Deploying the Murmansk-BN Electronic Warfare System to the Kaliningrad Region." *Izvestiya Online*, April 26, 2019.

Stepanov, Aleksandr. Interview with Yuriy Illarionovich Lastochkin. "They Have Deployed a Dome Which Defends from Missiles Over the Russian Bases in Syria." *MK Online*, April 15, 2018.

TAdviser. "Bylina System RB-109A." September 29, 2017.

Thomas, Timothy. *Advanced Weaponry and Russian Military Art of War*. MITRE, September 2020. https://www.mitre.org/.

———. *Russia's Electronic Warfare Force: Blending Concepts with Capabilities*. McLean, VA: MITRE, September 2020. https://www.mitre.org/.

Trevithick, Joseph. "Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio Virus." *The War Zone*, October 30, 2019. https://www.twz.com/.

Wasielewski, Philip G. "The Roots of Russian Military Dysfunction." *Foreign Policy Research Institute*, March 31, 2023. https://www.fpri.org/.

Withington, Thomas. "Russian Radiation." *Armada International*, November 10, 2022. https://www.armadainternational.com/.

THE INTELLECTUAL AND LEADERSHIP CENTER OF THE AIR FORCE

AIR UNIVERSITY

AUP

AIR UNIVERSITY PRESS

https://www.airuniversity.af.edu/AUPress/

ISSN 2687-7260