Return of Ground-Based Electronic Warfare Platforms and Force Structure

Maj. Morgan J. Spring-Glace, U.S. Army

The U.S. military is not achieving overmatch against the Russian military, as Timothy Bonds of the RAND Corporation testified to the House Armed Services Committee's Subcommittee on Tactical Air and Land Forces in 2017. The testimony cited Russian capability modernization and force availability as the contributors to losing overmatch. Of the capability modernization, Bonds specified new systems or improvements to existing systems among tanks, artillery, fixed- and rotary-wing aircraft, sophisticated and tiered air defense networks, long-range missiles, and cyberspace and electromagnetic warfare capabilities.[1]

Most of these capabilities also reside in the current force of the U.S. Army, and modernization efforts are ongoing to mitigate disparities. However, some capabilities,

most notably electronic warfare (EW), specifically electronic attack (EA), were culled from the U.S. Army between the end of the Cold War and the building of the BCT-centric Army for Iraq and Afghanistan. While the Army retains some of its EW capability in the form of signals intelligence (SIGINT, also known as EW support), EA systems such as the AN/MLQ-34 TACJAM and the AN/TLQ-17A TRAFFIC JAM were taken out of the inventory with no replacement, and formations dedicated to providing functional support to combat brigades and divisions were inactivated. These drawdowns were made under the assumption that Army forces can rely on their joint partners for EA capabilities. However, Field Manual 3-0, *Operations*, and Training and Doctrine Command Pamphlet 525-3-8, *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045*, state that all domains will be contested, and the Army cannot continuously rely on joint partners when faced with peer and near-peer competitors such as Russia or China, both of which are capable of challenging U.S. air and electromagnetic superiority.[2] Since the bulk of current U.S. EA capability resides in the U.S. Air Force and the U.S. Navy, and Chinese and Russian capability contests the other services' ability to support Army forces, how can the Army reliably benefit from EA capability? One answer is that the U.S. Army must bring back ground-based EA and deception platforms, and requisite force structure. This is necessary to mitigate the gap in overmatch that U.S. Army forces are currently facing.

Peer Adversary Electronic Warfare Capability

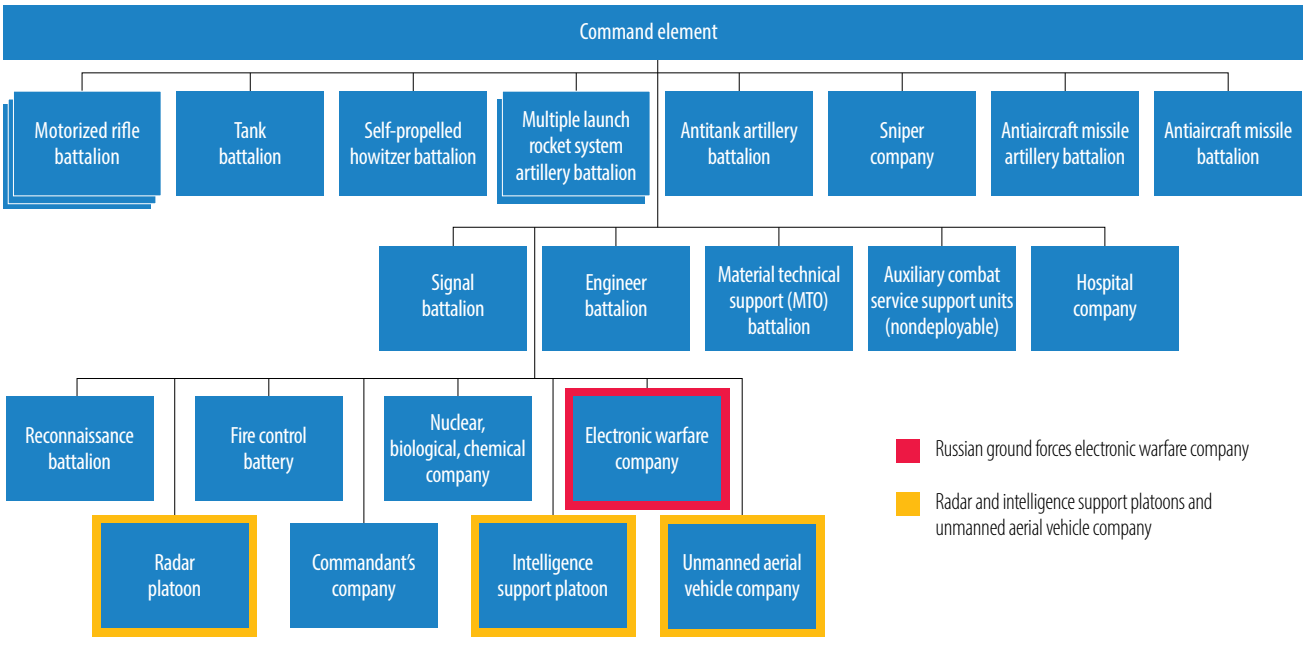
Russia, China, Iran, and North Korea possess peer or near-peer military capability, and other states possess aspects of that level of threat. To understand the gap between U.S. EA capability and peer adversaries, we will primarily examine Russia.

Russia is able to integrate cyberspace and EW capabilities across the tactical, operational, and strategic levels. At the strategic and operational levels, Russia has organized five total EW brigades, with two EW brigades in its Western Military District. This allocation is only from the Russian Ground Forces (RGF) and does not include the Russian navy and air force EW units.[3] Operational and strategic RGF EW forces seek to confuse and deceive opposing force military decision-makers at all levels. This is achieved by combining cyberspace and information warfare capabilities while also protecting operational-level assets and preventing access to an area of conflict by integrating air defense capability as part of an anti-access/area-denial strategy.[4] Each RGF EW brigade consists of four EW battalions, which can accomplish operational and strategic tasks or support smaller RGF units such as divisions or lower.[5]

At the tactical level, the RGF maneuver brigades have an EW company, an unmanned aircraft systems (UAS) company, and an intelligence support platoon (see figure, page 43).[6] Within an EW company are twelve vehicle-mounted EW platforms and fifteen man-portable jammers staffed with approximately one hundred personnel.[7] Each of the truck-mounted jammers have a different function, and the RGF EW company provides an array of communications, radar, and other jamming capabilities to the brigade commander. Each RGF EW company can electronically locate targets; jam and disrupt high frequency, very-high frequency, and ultra-high frequency communications; and jam, disrupt, or deceive GPS, to include mimicking GPS location/timing and other disruptions to UAS common data link, which can compromise or hijack most UAS.[8] They can jam ground, airborne, and maritime radars up to a range of three hundred kilometers and introduce false targets. RGF EW systems can also jam various aircraft navigation systems for manned and unmanned platforms.[9] Some systems can defeat proximity fuses in rockets and artillery or jam S-, X- and Ku-band radars, which includes U.S. Army artillery-locating and air defense radars, and airborne platforms such as the airborne warning and control system as well as radar-guided missiles.[10]

The Russian military has a long history of successful use of EW, whether disrupting and neutralizing sensors and communications or pairing SIGINT to artillery systems. During the initial phases of the Russian invasion of Georgia, the Russian air force lost five aircraft to Georgian air defense systems until the RGF deployed ground-based jamming platforms.[11]

Previous page: A new Electronic Warfare Tactical Vehicle (EWTV) takes part in test exercises 16 January 2018 at Yuma Proving Grounds, Arizona. The EWTVs were developed in response to an operational requirement to sense and jam enemy communications and networks. The Army's Rapid Equipping Force began introducing the EWTV into Army units at the end of 2018. (Photo by Mark Schauer, U.S. Army)



(Original figure by Roger N. McDermott; adapted by author)

Figure. Russian Ground Forces Motorized Rifle Brigade Structure

In 2014, Russian-backed Ukrainian separatists benefitted from Russian EW as demonstrated by the successful disruption of Ukrainian military UAS and proximity-fused Ukrainian artillery munitions at various ranges between 1 km and 30 km for ground forces and up to 240 km for Ukrainian air systems.[12] Additionally, Ukrainian military communications were significantly disrupted by multiple EW systems deployed for interlocking, mixed-system jamming and EW support coverage, aiding both EW and artillery.[13] In Syria, the Russians deployed the Krasukha-4 jamming system, leading to the successful jamming of U.S. communications and sensors. According to Gen. Raymond Thomas, former commander of U.S. Special Operations Command, Syria became "the most aggressive electromagnetic environment in the world."[14]

U.S. Electronic Warfare Capability

Unlike the Russian military, which retained and modernized its EW and EA capabilities, the U.S. Army culled a number of capabilities and formations, to include EA and EW formations, to build the modular Army. As a result, the Army became reliant on joint partners for a number of capabilities to include EA.

The Army retained SIGINT capability, which is designed to provide SIGINT to brigade combat teams (BCTs). The Army's experience with improvised explosive devices in Iraq and Afghanistan prompted the fielding of counter remote-controlled improvised explosive devices and counter remote-controlled EW devices, protecting a single ground patrol from radio-controlled improvised explosive device threats.[15] The Army also equipped rotary-wing aircraft with aircraft survivability equipment as a countermeasure to shoulder-fired surface-to-air missiles.[16] Though counter remote-controlled EW devices and aircraft survivability systems are EA systems, they are defensive in nature, as each system's purpose is to protect an asset. When the Army needs to offensively employ EA to disrupt enemy communications, neutralize sensors, or conduct electronic deception, the Army is reliant on its joint partners.

On the other hand, the U.S. Marine Corps

Maj. Morgan J. Spring-Glace, U.S. Army, is a military intelligence officer in the Combined Arms Doctrine Directorate at Fort Leavenworth, Kansas. He holds a BS in mechanical engineering from Worcester Polytechnic Institute and an MA in international relations from Webster University. He has served on the intelligence staff at the battalion, brigade, corps support, and theater levels.

Ground radio-electronic suppression module 1RL257E Krasukha-4 26 August 2015 at MAKS-2015 international aviation and space salon in the Moscow Region. The Krasukha-4 was reportedly used successfully in Syria to jam adversary communications to include those of U.S. and coalition forces. (Photo by Vitaly V. Kuzmin, www.vitalykuzmin.net)

has two ground-based EW systems, the AN/ULQ-19(V)2 EA set and the AN/MLQ-36 mobile EW support system. While the AN/MLQ-36 is an electronic support system and the AN/ULQ-19 is an EA system, the U.S. Marine Corps has less than nine EA platoons organized into three radio battalions.[17] However, this is meant to support the three Marine expeditionary forces and lacks the capacity to provide ground-based EA to the joint force. All other U.S. military EA assets, such as the Navy and U.S. Marine Corps EA-18 Growler aircraft or the U.S. Air Force EC-130H Compass Call, are airborne platforms. This refers back to the earlier statement that U.S. forces cannot guarantee air superiority and naval access to support ground forces in future conflicts.[18] So, the shortage in ground-based EW, specifically, is ground-based EA capability.

There is some movement on bringing back ground-based EW in the Army, such as the U.S. Army Europe efforts to field systems to EW personnel in BCTs and similar programs and initiatives to provide EA capability and bolster ES capability, which provide vehicle-mounted, man-portable, rotary-wing-mounted, and UAS-mounted systems.[19] Other efforts include the Army bolstering cyberspace-electromagnetic activities staff to plan and synchronize EW operations within corps, divisions, and BCTs, which is also necessary to deconflict EW with communications and SIGINT.[20] The Army is also considering creating synergy between EW and SIGINT by using a common EW/SIGINT platform.[21]

However, the Army must take great care when implementing a solution for EW capability so that SIGINT and EW do not struggle over resources. While the Army can save money by fielding one vehicle to serve both SIGINT and EA interests (the terrestrial layer system), the formations should be kept separate so that one does not subsume the other. Matching our peer threat's capacity would require a company-sized organization in each combat brigade, manned and equipped for EA and separate from SIGINT capability and capacity within

the brigade. Even though the Army's new terrestrial layer system is a multipurpose, ground-based SIGINT/EA platform, when it comes down to troops-to-task, it can still only handle either EA or SIGINT at any given time.[22] While one jammer cannot neutralize another (though multiple jammers can use their direction-finding capabilities to locate a threat jammer and destroy it with artillery), threat overmatch in this context is the threat's ability to disrupt and neutralize communications and sensors without U.S. capability or capacity to do the same, granting significant advantage to the enemy. The U.S. Army does not benefit from matching system versus system; however, the U.S. Army will benefit from having the capacity to disrupt or neutralize more threat communications and sensors than the threat can affect or detect. Given the RGF combat brigade has three artillery battalions compared to one artillery battalion in a U.S. BCT, it behooves a U.S. BCT to disrupt or neutralize threat fires communication networks and sensors, which would require a dedicated EA formation in addition to separate ground-based SIGINT assets within each BCT.[23]

Conclusion

U.S. Army forces are currently facing overmatch gaps against peer or near-peer threats such as China and Russia. Creating EW platoons in military intelligence companies within BCTs and EW companies in expeditionary military intelligence brigades implies that the Army will have less EA capacity than its adversaries, such as the RGF with an EW company in each combat brigade, not to mention the EW brigades organized under the military districts.[24] This leaves the U.S. Army at a disparity of EA capability and capacity. Achieving a more advantageous ratio of U.S. ground-based EA forces and systems could involve creating EW companies within BCTs or separate EW battalions and brigades assigned to divisions or corps. While the projected force structure and systems will somewhat mitigate the overmatch, the Army cannot continuously rely on joint partners when faced with peer and near-peer competitors like Russia or China, who are capable of challenging U.S. air and electromagnetic superiority.[25] ■

Notes

1. Timothy M. Bonds, *Limiting Regret: Building the Army We Will Need-An Update: Addendum* (Santa Monica, CA: RAND Corporation, 2017), 4.

2. Field Manual (FM) 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office [GPO], 2017), 1-5–1-6 and 2-6; Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-8, *U.S. Army Concept: Multi-Domain Combined Arms Operations at Echelons Above Brigade 2025-2045, Versatile, Agile, and Lethal* (Fort Eustis, VA: TRADOC, 2018), 2, accessed 1 April 2019, https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-8.pdf; *The Most Significant Threats to U.S. Naval Forces and How U.S. Naval Forces Plan to Operate in a Contested Environment, Before the Committee on Armed Services, Subcommittee on Seapower*, 116th Cong. (2018) (statement *of* Mark T. Esper, Secretary of the Army, and Gen. Mark A. Milley, Chief of Staff).

3. Roger N. McDermott, *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum* (Tallinn, Estonia: International Centre for Defence and Security, 2017), 6–8, accessed 1 April 2019, https://icds.ee/wp-content/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

4. *Russia Military Power: Building a Military to Support Great Power Aspirations* (Washington, DC: Defense Intelligence Agency, 2017), 32 and 42; *Multi-Domain Combined Arms Operations*, 6; James Andersen, "Russian Artillery: Adapting Ancient Principles to Modern Paradigms, Part 2," *Red Diamond* 8, no. 11 (November 2017): 21–22 and 25–27.

5. McDermott, *Russia's Electronic Warfare Capabilities,* 6.

6. Ibid.

7. Ibid., 7; *Russia Military Power*, 53.

8. Jaysen A. Yochim, "The Vulnerabilities of Unmanned Aircraft System Common Data Links to Electronic Attack" (master's thesis, Weber State University, Ogden, UT, 2010), 40–41; Thomas E. Hay, "Determining Electronic and Cyber Attack Risk Level for Unmanned Aircraft in a Contested Environment" (master's thesis, Air University, Maxwell Air Force, AL, 2016), 5.

9. McDermott, *Russia's Electronic Warfare Capabilities,* B-1; Andersen, "Russian Artillery," 22.

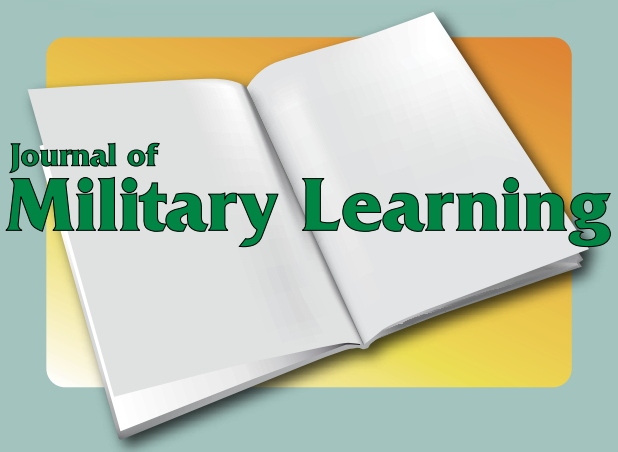
10. McDermott, *Russia's Electronic Warfare Capabilities,* B-1; "AN/TPQ-37 Firefinder Weapon Locating System," Thales-Raytheon Systems, May 2003, accessed 1 April 2019, http://www.radartutorial.eu/19.kartei/04.battle/pubs/cms01_050672.pdf; "AN/TPQ-53 Firefinder Weapon Locating Radar," Card Index of Radar Sets–Battlefield Radars, Radartutorial.eu, accessed 1 April 2019, http://www.radartutorial.eu/19.kartei/04.battle/karte013.en.html; "Sentinel Aerial Surveillance Radar- AN/MPQ-64," U.S. Army Acquisition Support Center, accessed 1 April 2019, https://asc.army.mil/web/portfolio-item/anmpq-64-sentinel/; "1L269 Krasukha-2," Tactical Vehicles, Deagel, updated 7 April 2017, accessed 1 April 2019, http://www.deagel.com/Tactical-Vehicles/1L269-Krasukha-2_a003129001.aspx.

11. Andersen, "Russian Artillery," 22; Lester W. Grau and Charles K. Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces* (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), 289.

12. "Dr. Phillip Karber Explains Russian Operations in Ukraine," YouTube video, 27:39, posted by "Modern War Institute," 13 April 2017, accessed 1 April 2019, https://www.youtube.com/watch?v=14LMmBsDw-g.

13. McDermott, *Russia's Electronic Warfare Capabilities,* 26.

CALL FOR PAPERS



The *Journal of Military Learning* (*JML*) is a peer-reviewed semiannual publication that supports the military's effort to improve education and training for the U.S. Army and the overall profession of arms. The *JML* invites practitioners, researchers, academics, and military professionals to submit manuscripts that address the issues and challenges of adult education and training, such as education technology, adult learning models and theory, distance learning, training development, and other subjects relevant to the field. Book reviews of published relevant works are also encouraged.

To view the current and past editions of the *JML*, visit Army University Press at https://www.armyupress.army.mil/Journals/Journal-of-Military-Learning/.

We are now accepting manuscripts for future editions of the *JML*. Manuscripts should be submitted to usarmy.leavenworth.tradoc.mbx.journal-of-military-learning@mail.mil. Submissions should be between 3,500 and 5,000 words and supported by research, evident through the citation of sources. For detailed author submission guidelines, visit the *JML* page on the Army University Press website at https://www.armyupress.army.mil/Journals/Journal-of-Military-Learning/April-2017-Edition/Author-Submission-Guidelines/.

For additional information, call 913-684-5429 or send an email to the address above.

14. Douglas Barrie and Howard Gethin, *Russian Weapons in the Syrian Conflict* (Rome, Italy: NATO Defense College, 2018), 7; Anya Loukianova, *Moscow's Emerging Electronic Warfare Capabilities: a Dangerous Jammer on U.S./NATO-Russian Relations?* (Program on Strategic Stability Evaluation: Georgia Institute of Technology, Atlanta, 2016), 9; "Keynote: Gen. Raymond A. Thomas III, Commander, U.S. Special Operations Command," Vimeo video, 9:20, posted by "Trajectory on Location," in Joseph Trevithick, "American General Says 'Adversaries Are Jamming AC-130 Gunships in Syria," The Drive, 25 April 2018, accessed 1 April 2019, http://www.thedrive.com/the-war-zone/20404/american-general-says-adversaries-are-jamming-ac-130-gunships-in-syria.

15. Michael E. Pesci, "Systems Engineering in Counter Radio-Controlled Improvised Explosive Device Electronic Warfare," *Johns Hopkins APL Technical Digest* 31, no. 1 (2012): 59.

16. Army Techniques Publication 3-36, *Electronic Warfare Techniques* (Washington, DC: U.S. GPO, 2014), C-1.

17. Marine Corps Reference Publication 2-10A.1, *Signals Intelligence* (Washington, DC: U.S. GPO, 2016), 4-2; "1st Radio Battalion," U.S. Marine Corps, accessed 1 April 2019, https://www.imef.marines.mil/Units/I-MIG/1ST-RADIO-BN/; "2nd Radio Battalion," U.S. Marine Corps, accessed 1 April 2019, https://www.iimef.marines.mil/Units/2nd-Radio-Battalion/; "3d Radio Battalion," U.S. Marine Corps, accessed 1 April 2019, https://www.iiimef.marines.mil/Units/III-MIG/Commands/3RadBn/.

18. Loukianova, *Moscow's Emerging Electronic Warfare Capabilities,* 10; Hay, "Determining Electronic and Cyber Attack Risk Level," 1-2; TP 525-3-8, *Multi-Domain Combined Arms Operations*, 6.

19. Nancy Jones-Bonbrest, "Electronic Warfare Prototypes Improve Operational Understanding Against Near-Peer Threats," Army Rapid Capabilities and Critical Technologies Office, 10 May 2018, accessed 1 April 2019, http://rapidcapabilitiesoffice.army.mil/news/Electronic-warfare-prototypes-improve-operational-understanding/; Justin Lynch, "The Army Prepares for 'Irregular Warfare,'" Fifth Domain, 11 June 2018, accessed 1 April 2019, https://www.fifthdomain.com/dod/army/2018/06/11/the-army-prepares-for-irregular-warfare/; Dan Goure, "Gen. Milley Is Right: The US Army Is On the Mend," Defense News, 13 June 2018, accessed 1 April 2019, https://www.defensenews.com/land/2018/06/13/gen-milley-is-right-the-us-army-is-on-the-mend/.

20. Sydney J. Freedberg Jr., "Army Boosts Electronic Warfare Numbers, Training, Role," Breaking Defense, 7 August 2018, accessed 1 April 2019, https://breakingdefense.com/2018/08/army-boosts-electronic-warfare-numbers-training-role/.

21. Sydney J. Freedberg Jr., "Army Wrestles With SIGINT vs. EW," Breaking Defense, 31 July 2018, accessed 1 April 2019, https://breakingdefense.com/2018/07/army-wrestles-with-sigint-vs-ew/.

22. Ibid.

23. *Russia Military Power*, 53.

24. Freedberg, "Army Boosts Electronic Warfare Numbers, Training, Role."

25. FM 3-0, *Operations,* 1-5–1-6 and 2-6; TP 525-3-8, *Multi-Domain Combined Arms Operations*, 2.