Ground Electronic Warfare: Background and Issues for Congress

September 17, 2019

Congressional Research Service
https://crsreports.congress.gov
R45919

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R45919

September 17, 2019

John R. Hoehn
Analyst in Military Capabilities and Programs

Ground Electronic Warfare: Background and Issues for Congress

Ground electronic warfare (EW) is a group of programs directed by the Army and Marine Corp which are designed to effect ground forces use of the electromagnetic spectrum. The U.S. military has several ground EW programs that are used for different missions. These programs can broadly be categorized into counter-improvised explosive device (C-IED) systems, counter-unmanned aerial systems (C-UAS), and communications and radar jammers. Over the past several years, senior leaders in the Army and Marine Corps have testified about the need to improve EW capabilities.

Role of EW in Ground Operations

EW is a component of modern warfare, particularly in response to threats posed by potential adversaries such as Russia and China. EW refers to operations that use the electromagnetic spectrum (i.e., the "airwaves") to detect, listen to, jam, and deceive (or "spoof") enemy radars, radio communication systems, data links, and other electronic systems. EW also refers to operations that defend against enemy attempts to do the same.

Ground EW programs have gained importance in an era of "great power competition." Countries like Russia and China have developed so-called anti-access/area denial (A2/AD) systems, some of which are designed to prevent U.S. military access to radio and satellite communications, and to deny the use of radars for artillery and air defense operations.

Ground Forces EW Programs

This report focuses on three categories of unclassified EW programs in the Army and Marine Corps, along with their respective programs and systems:

- **Counter-IED:** the Thor and Duke Version III systems.
- **Counter-UAS:** the Batelle Drone Defender, Blighter Counter-UAS system, the Mobile Expeditionary High Energy Laser, the Marine Air Defense Integrated System (MADIS), and the Compact Laser Weapons System (CLaWS).
- **Communications and radar jammers:** the EW Tactical Vehicle (EWTV), the EW Planning and Management Tool (EWPMT), the Communication Emitter Sensing and Attacking System II (CESAS II), and the Mobile EW Support System (MEWSS).

Potential Oversight Issues for Congress

Congress has continually shown interest in EW, and the decisions it makes regarding EW could affect future military capabilities and funding requirements. In particular, EW programs pose several potential issues for Congress:

- Is DOD's proposed mix of ground EW capabilities and investments appropriate?
- How do the Army and Marine Corps transition emerging technologies from demonstrations into programs, and are these programs funded adequately?
- What role might emerging technologies have in shaping current EW plans and programs?

Contents

Figures

Appendixes

Contacts

Introduction

This report focuses on selected ground electronic warfare (EW) systems.[1] The Department of Defense (DOD) FY2020 budget requests funding for a number of ground EW systems associated with the Army and the Marine Corps.

Generally, ground EW capabilities seek to use the electromagnetic spectrum to achieve one of three battlefield effects. First, ground EW systems can be used to defeat Improvised Explosive Devices (IED). This was the focus of the U.S. military's ground EW programs for the past decade and a half. A second role for ground EW can be to defeat Unmanned Aerial Systems (UAS). A third role, largely a legacy from the Cold War, can be to jam enemy communications and radars.

An overall issue for Congress is whether to approve, reject, or modify DOD's proposals for ground EW programs. These programs also pose a number of potential oversight issues for Congress. Congress's decisions on these issues could affect future U.S. military capabilities and funding requirements. Potential issues for Congress include

- balancing EW programs between counter-improvised explosive device missions and great power competition,
- potentially standardizing how different services approach EW funding, and
- the role new technologies may play in EW operations.

Background

EW Overview[2]

Electronic warfare (EW)—sometimes also called electromagnetic maneuver warfare (EMW)[3]—is an integral component of modern warfare, particularly in operations against technologically sophisticated potential adversaries such as Russia and China. EW generally refers to operations that use the electromagnetic spectrum (i.e., the "airwaves") to detect, listen to, jam, and deceive (or "spoof") enemy radars, radio communication systems and data links, and other electronic systems. EW also refers to operations for defending against enemy attempts to do the same. More formally, DOD defines electronic warfare as "[m]ilitary action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy."[4]

[1] This report focuses on Army and Marine Corps ground electronic warfare systems. For a discussion of U.S. airborne electronic attack systems, see CRS Report R44572, *U.S. Airborne Electronic Attack Programs: Background and Issues for Congress*, by John R. Hoehn.

[2] For a brief overview of EW, see CRS In Focus IF11118, *Defense Primer: Electronic Warfare*, by John R. Hoehn.

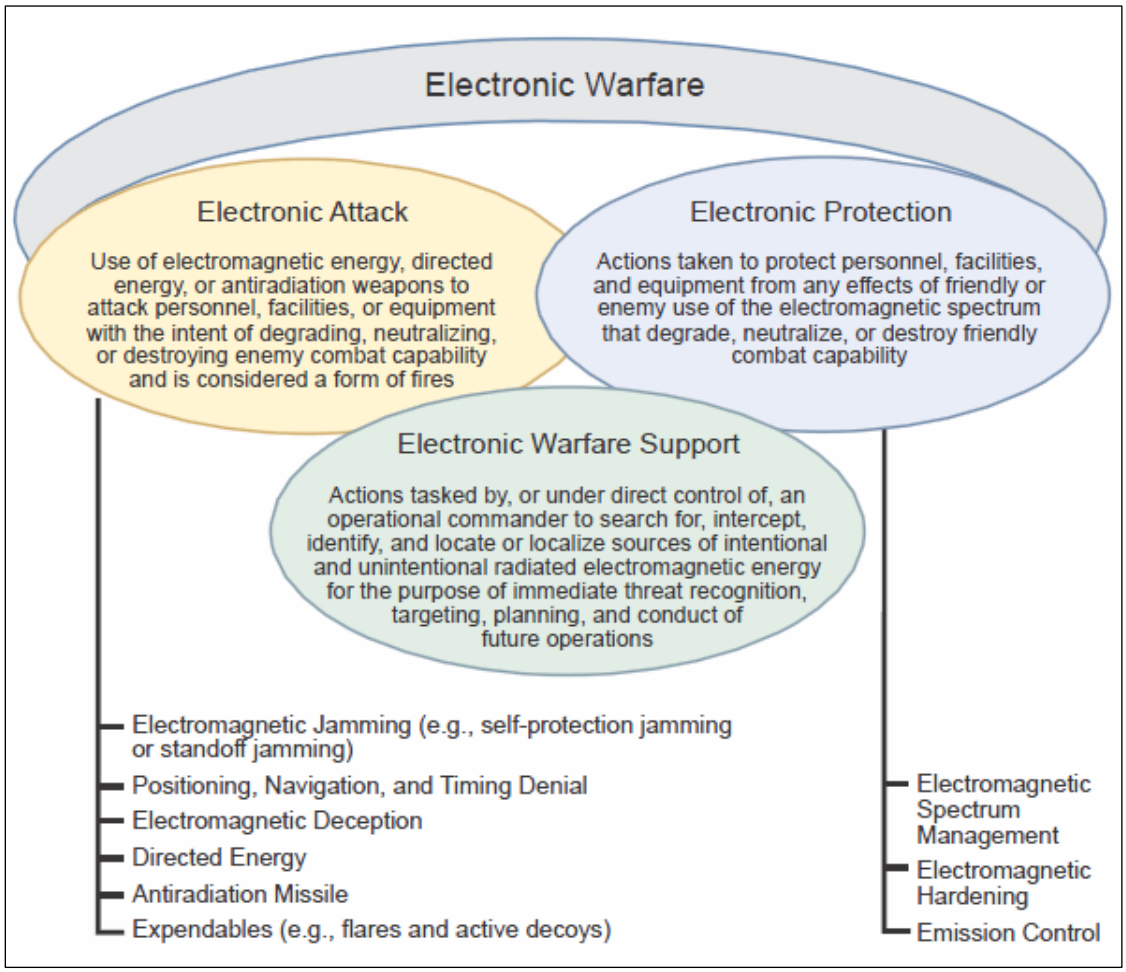
[3] See, for example, John Joyce, "Navy Expands Electromagnetic Maneuver Warfare for 'Victory at Sea,'" *Navy News Service*, November 2, 2017; Robert K. Ackerman, "Electromagnetic Maneuver Warfare Looms as New U.S. Navy Discipline," *Signal*, February 11, 2015.

[4] Department of Defense, *DOD Dictionary of Military and Associated Terms As of February 2019*, p. 78, accessed March 13, 2019, at https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf. See also Department of Defense, *Joint Publication 3-13.1, Electronic Warfare*, February 8, 2012, 144 pp. (including covers), accessed March 13, 2019, at https://www.globalsecurity.org/military/library/policy/dod/joint/jp3_13_1_2012.pdf and https://publicintelligence.net/jcs-ew/.

As shown in **Figure 1**, DOD divides EW into electronic warfare support, electronic protection, and electronic attack. *Electronic warfare support*, sometimes also referred to as electronic support measures (ESM), involves listening to an adversary's radar and radio transmissions in an attempt to detect, locate, and understand how to avoid, jam, or deceive those systems. *Electronic protection* involves limiting the electromagnetic signatures of one's own military equipment and hardening one's own military equipment against the effects of enemy EW operations. *Electronic attack* (EA) involves jamming and deceiving enemy radars and radio communications and data links.

Developing ever-better EW systems is a component of the competition in military capabilities between major military powers. Because EW programs tend to be classified and are sometimes related to intelligence systems and capabilities, these systems are not frequently discussed publicly in much detail.

Figure 1. Overview of Electronic Warfare



Source: Department of Defense, *Joint Publication 3-13.1, Electronic Warfare*, February 8, 2012, Figure I-3, on p. I-5, accessed March 13, 2019, at https://www.globalsecurity.org/military/library/policy/dod/joint/jp3_13_1_2012.pdf and https://publicintelligence.net/jcs-ew/.

Ground EW systems provide EW support, electronic protection, and electronic attack. For instance, the Marine Corps' Mobile Electronic Warfare Support System categorizes enemy radio signals. Many of the counter-improvised explosive device countermeasures serve in both a

protection and attack role by emitting a signal to jam radio communications to "attack" communications while protecting soldiers and marines. Counter-unmanned aerial systems provide a similar function for drones.

U.S. Military Ground EW Programs

Counter-Improvised Explosive Device (C-IED)

In the immediate post-Cold War era, electronic warfare gained prominence as a potential way to mitigate threats from improvised explosive devices (IEDs). During counter-insurgency operations in Iraq and Afghanistan, U.S. and allied ground forces suffered many casualties from IEDs. To detonate IEDs, insurgents learned to use cell phones, small two-way radios, and other basic radio communications to maximize the amount of damage. One C-IED method the DOD developed was for EW systems to jam IED communications radio frequencies to prevent them from detonating. From FY2006 through FY2011, the Joint IED Defeat Organization received $18 billion to develop C-IED technologies, including electronic warfare systems.[5]

These C-IED techniques included the development of a "man-portable" platform (see **Figure 2**), which supports U.S. forces on foot patrol, without the protection of a vehicle. However, due to power constraints, these types of C-IEDs provide jamming in a limited area; the jammers use batteries that are heavy and must be carried. DOD also procured C-IED jamming systems for vehicles, such as the Duke Version 3 system (**Figure 3**), which can be installed on nearly any vehicle, though typically it is installed on the Humvee or the Mine-Resistant Ambush Protected Vehicle. Although these vehicular-based C-IED jammers are more powerful, because they draw power from the vehicle's engine, they are not able to accompany ground forces into buildings or in constricted areas such as alleyways. Thus ground forces require both systems, for mounted (travelling by vehicle) and dismounted (travelling by foot) operations.

Figure 2. Thor Man-Portable Counter-IED Device

Source: https://en.wikipedia.org/wiki/Counter-IED_equipment#/media/File:Two_Soldiers_operate_Thor_and_Minehound.jpg.

[5] U.S. Government Accountability Office, *Counter-Improvised Explosive Devices: Multiple DOD Organizations are Developing Numerous Initiatives*, GAO-12-861R, August 1, 2012, https://www.gao.gov/assets/600/593242.pdf. This dollar figure does not reflect C-IED spending from the Army, Navy, Marine Corps, and Air Force.

Notes: The image caption reads, "Two soldiers with the 25th Infantry Division operate Thor and Minehound, two counter-IED devices." The Thor system in this picture is backpack-like device on the soldier on the right.

Figure 3. Duke Version 3 Vehicle Mounted CREW system

Source: https://www.srcinc.com/what-we-do/ew/crew-duke.html.

Counter-Unmanned Aerial Systems (C-UAS)

The emergence of unmanned aerial systems (UAS), more commonly called drones, has created unique challenges for U.S. military forces. Both state and nonstate actors have employed drones for intelligence, surveillance, and reconnaissance (ISR) and certain strike capabilities (particularly large UAS platforms such as the MQ-9 Reaper for U.S. allies or the Wing Loong II developed by the People's Republic of China). Most UAS systems use radio frequencies to operate.

Adversaries have used UAS to support ground operations in recent years. The Islamic State (IS, also known as Islamic State in Iraq and the Levant (ISIL)) modified commercial drones to perform reconnaissance and drop small explosives, such as hand-grenades and mortars, on unsuspecting personnel.[6] The Russian military demonstrated its ability to pair EW drones with artillery fire, with devastating effects. According to U.S. intelligence sources, Russian forces used a single drone to provide intelligence for an artillery fire mission in July 2014 that resulted in the destruction of two Ukrainian battalions within minutes.[7] Emerging concepts like "swarming," where many small drones work together to accomplish a task, are also being developed. In 2015, IS demonstrated swarming tactics to attack a Russian airbase in Syria—though it is unclear how effective these swarming tactics were against Russian forces.[8]

[6] For example, see Joby Warrick, "Use of weaponized drones by ISIS spurs terrorism fears," *Washington Post*, February 21, 2017, at https://www.washingtonpost.com/world/national-security/use-of-weaponized-drones-by-isis-spurs-terrorism-fears/2017/02/21/9d83d51e-f382-11e6-8d72-263470bf0401_story.html?utm_term=.99d621cffba3.

[7] Samuel Cranny-Evans, Mark Cazalet, and Christopher F Foss, "The Czar of battle: Russian artillery use in Ukraine portends advances," IHS Jane's, April 24, 2018, at https://janes.ihs.com/Janes/Display/FG_901376-IDR.

[8] For example, see David Axe, "How Russia Says It Swatted Down a Drone Swarm in Syria," *Vice News*, January 12, 2018, at https://www.vice.com/en_us/article/43qbbw/russia-says-it-swatted-down-drone-swarm-syria-isis; Kyle Rempfer, "Did US drones swarm a Russian base? Probably not, but that capability isn't far off.," *Military Times*, October 29, 2018, at https://www.militarytimes.com/news/2018/10/29/did-us-drones-swarm-a-russian-base-probably-

As a result, DOD has developed EW techniques to deny potential adversaries the ability to use drone aircraft. These counter-UAS systems are divided into two categories: systems that detect UAS, and systems that interdict UAS systems kinetically or nonkinetically. Some counter-UAS systems are capable of both detection and attack. According to one analyst, as of February 2018 there were 235 counter-UAS products from 155 manufacturers.[9] These counter-UAS products range from hand-held devices that can jam radio and global positioning system (GPS) signals for point defense (see **Figure 4**) to larger, ground-based systems that can defend larger areas (see **Figure 5**). The latest generation of counter-UASs by the Army and Marine Corps are being developed to destroy targets using directed energy such as lasers.[10]

Figure 4. Battelle Drone Defender Counter UAS Device

Source: https://www.battelle.org/government-offerings/national-security/payloads-platforms-controls/counter-UAS-technologies/dronedefender.

Note: The Battelle Drone Defender is capable of jamming regular radio frequencies as well as GPS. The Drone Defense has a range of 400 meters.

not-but-that-capability-isnt-far-off/.

[9] Arthur Holland Michel, *Counter-Drone Systems*, Center for the Study of Drones, Annandale-on-Hudson, NY, February 2018, https://dronecenter.bard.edu/files/2018/02/CSD-Counter-Drone-Systems-Report.pdf.

[10] Sydney J. Freedberg Jr., "It's Raytheon Vs. Dynetics/Lockheed for Army's 100 kW Laser," *Breaking Defense*, August 10, 2018, at https://breakingdefense.com/2018/08/its-raytheon-vs-dynetics-lockheed-for-armys-100-kw-laser/.

Figure 5. Blighter Counter-UAS System

Source: https://asianmilitaryreview.com/2019/05/counter-uav-high-tech-flyswatters/.

Notes: The Blighter Counter-UAS is reported to be used at commercial airports in the United Kingdom.

The Army has recently developed vehicle-mounted lasers capable of engaging UAS. In 2018, the Army tested the Mobile Expeditionary High Energy Laser (MEHEL), a 5 kilowatt (kW) laser, which is placed on a Stryker-armored vehicle (see **Figure 6**). This laser has demonstrated being capable of destroying small drones in flight.[11] The Army is planning to test a more powerful 10kW laser, and anticipates upgrading to a 50 kW laser,[12] capable of destroying rockets, artillery, and mortars, by 2022.[13] The Army plans to translate these technology demonstrators into future air defense systems by the mid-2020s. However, several challenges remain for the Army to field laser technologies. The first challenge is to develop a sufficient energy source that can fit into relatively small spaces.[14] Some of the first lasers required a large power source housed in a semi-truck trailer—a power system too large to be practical for operational forces. The second challenge is providing sufficient power so that a laser beam can travel long distance.[15] Light

[11] The MEHEL's maximum range is not publically available. Sydney J. Freedberg Jr., "Drone-Killing Laser Stars In Army Field Test," *Breaking Defense*, May 11, 2017, at https://breakingdefense.com/2017/05/drone-killing-laser-stars-in-army-field-test/.

[12] The Army maintains a series of power generators under the AMMPS program. The largest of which is a 60 kW generator which is capable of powering a large house or a small factory.

[13] Dr. Kip R. Kendrick, "Army looks to optimize lethality with high-energy lasers," *U.S. Army*, February 8, 2018, at https://www.army.mil/article/200308/army_looks_to_optimize_.

[14] Ashley Roque, "*Around the corner: Directed-energy technology's last hurdles*," IHS Janes, June 19, 2019, at https://janes.ihs.com/Janes/Display/FG_2085727-IDR.

[15] Ashley Roque, *"Around the corner: Directed-energy technology's last hurdles,"* IHS Janes, June 19, 2019, at https://janes.ihs.com/Janes/Display/FG_2085727-IDR.

quickly diffuses in the atmosphere, thereby limiting the range of the system, particularly for lower-powered lasers.

Figure 6. The Mobile Expeditionary High-Energy Laser Attached to a Stryker-Armored Vehicle

Source: https://www.uasvision.com/2019/05/09/us-army-to-put-laser-weapon-on-stryker-combat-vehicles/.

Notes: The image caption reads, "A Stryker combat vehicle equipped with a 5-kW laser and an array of sensors shot small fixed- and rotary-wing UAS in April during MFIX-17 at Fort Sill."

Similarly to the Army, the Marine Corps is developing its own counter-UAS systems through the ground-based air defense (GBAD) program. In June 2019, the Marine Corps Warfighting Lab announced the first laser-approved operations, named the Compact Laser Weapons System (CLaWS) (see **Figure 7**). According to the Marine Corps, the CLaWS program is a rapid prototyping effort to provide an affordable solution for the C-UAS challenge.[16] The Marine Corps is also procuring the Marine Air Defense Integrated System (MADIS) as part of its GBAD future weapons system. MADIS is a C-UAS system designed to be integrated onto the Joint Tactical Light Vehicle.[17] In the FY2020 budget request, the Marines requested procurement funding to integrate 28 MADIS systems into the service's vehicle fleet.[18]

[16] Ashley Calingo, "MARINE CORPS AT THE FOREFRONT FOR GROUND-BASED LASERS," *U.S. Marine Corps*, June 19, 2019, at https://www.marines.mil/News/News-Display/Article/1880583/marine-corps-at-the-forefront-for-ground-based-lasers/.

[17] L-MADIS was used in the Persian Gulf to engage Iranian drones in July 2019. For more information on the use of this system see Gina Harkins, "Here's the New Marine Corps Weapon that Just Destroyed an Iranian Drone," *Military.com*, July 18, 2019, at https://www.military.com/daily-news/2019/07/18/heres-new-marine-corps-weapon-just-destroyed-iranian-drone.html.

[18] Department of Defense FY2020 P-40 Budget Justification for Line Item 3006, Ground Based Air Defense (GBAD).

Figure 7. Marine Corps Compact Laser Weapons System

Source: https://www.marines.mil/News/News-Display/Article/1880583/marine-corps-at-the-forefront-for-ground-based-lasers/.

Notes: The image caption reads: "A Marine conducts pre-deployment training and evaluation. Additionally, Marines are evaluating the Compact Laser Weapons System, the first ground-based laser approved by the Department of Defense for use by warfighters, as another potential C-UAS defeat capability."

Communications Jamming

Advances in networking sensors and computing power have made using the electromagnetic spectrum for communications an important task in any military operation. These networks allow a military to develop a comprehensive picture of the battlespace and enable forces to effectively coordinate attacks. Disrupting an enemy's communications systems limits their ability to command forces and maintain battlespace awareness. Both the Army and the Marine Corps have developed several programs to deny potential adversaries access to their communications networks.

The Army's primary communications jammer is the EW tactical vehicle (EWTV), a modified mine-resistant ambush protected vehicle that incorporates a variant of the CREW Duke system (see **Figure 8**).[19] According to the Army, the EWTV was "developed to provide Army EW Teams with the ability to sense and jam enemy communications and networks from an operationally relevant range at the brigade combat team level."[20] The Army states that the EWTV is designed to provide electronic attack capabilities for brigade combat teams.

[19] Daniel Wasserbly, "US Army working to field new Electronic Warfare Tactical Vehicles," *Jane's*, IHS Markit, October 9, 2018, https://www.janes.com/article/83673/ausa-2018-us-army-working-to-field-new-electronic-warfare-tactical-vehicles.

[20] Daniel Wasserbly, "US Army working to field new Electronic Warfare Tactical Vehicles," *Jane's*, IHS Markit, October 9, 2018, https://www.janes.com/article/83673/ausa-2018-us-army-working-to-field-new-electronic-warfare-tactical-vehicles.

Figure 8. Army Electronic Warfare Tactical Vehicle (EWTV)

Source: https://www.thedrive.com/the-war-zone/23506/this-is-the-armys-new-electronic-warfare-vehicle-the-first-of-its-kind-in-years.

To manage electronic attack and electronic support capabilities, the Army uses the EW planning and management tool (EWPMT).[21] This system is often installed between the antennae and radio transceiver. The EWPMT allows operators to neutralize and exploit enemy signals through a computer program called Raven Claw. [22] The software gives EW commanders a comprehensive view of the electromagnetic spectrum, allowing them to detect and jam enemy communications systems and radars.[23]

Marine Corps radio battalions primarily employ the Communication Emitter Sensing and Attack System (CESAS) II to jam communications systems.[24] According to a project officer, the CESAS II "has the ability to operate in a larger frequency range, covering a much larger portion of the communications spectrum [high frequency, very high frequency, and ultra high frequency]."[25] CESAS II comes in two variants: a vehicle-transportable version (see **Figure 9**) and a man-

[21] "Electronic Warfare Planning and Management Tool (EWPMT)," *USAASC*, 2019, asc.army.mil/web/portfolio-item/iews-electronic-warfare-planning-and-management-tool-ewpmt/.

[22] "Electronic Warfare from a Laptop - Raytheon's Raven Claw Tool Helps the U.S. Army Own the EW Spectrum," *Raytheon*, 2018, http://www.raytheon.com/news/feature/electronic-warfare-laptop.

[23] "Electronic Warfare from a Laptop - Raytheon's Raven Claw Tool Helps the U.S. Army Own the EW Spectrum." *Raytheon*, 2018, http://www.raytheon.com/news/feature/electronic-warfare-laptop.

[24] Headquarters Marine Corps, "COMMUNICATIONS EMITTER SENSING AND ATTACKING SYSTEM II (CESAS II)" *U.S. Marine Corps Concepts & Programs*, http://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-2-Information-Operations/Part-22-ISR/CESAS-II/. Funding for CESAS II is contained in program element 0206625M *USMC Intelligence/Electronics Warfare Sys*, and Navy Line Item 4747 *Intelligence Support Equipment*.

[25] Marine Corps Systems Command, "Corps ready to wage electronic warfare with new mobile sensor, attack system," press release, September 7, 2016, https://www.marcorsyscom.marines.mil/News/News-Article-Display/Article/936029/corps-ready-to-wage-electronic-warfare-with-new-mobile-sensor-attack-system/.

portable system. According to Marine Corps Systems Command, CESAS II reduces the weight of the vehicle jammer from 1,300 pounds to 670 pounds; the man-portable version weighs 180 pounds. The Marine Corps declared initial operational capability in July 2016 and plans to declare full operational capability in FY2021.[26]

Figure 9. High Mobility Multipurpose Wheeled Vehicle Equipped with CESAS II

Source: https://www.marcorsyscom.marines.mil/News/News-Article-Display/Article/936029/corps-ready-to-wage-electronic-warfare-with-new-mobile-sensor-attack-system/.

The AN/MLQ-36 Mobile Electronic Warfare Support System (MEWSS) is another vehicle the Marine Corps uses to jam communications and other electronic transmissions—such as radar.[27] The Marine Corps fields 12 MEWSSs, which are modified light-armored vehicles procured in 1987.[28] The MEWSS has received a series of upgrades, including a program called the MEWSS Product Improvement Program, which added a 9-meter extendable mast.[29]

[26] Headquarters Marine Corps, "COMMUNICATIONS EMITTER SENSING AND ATTACKING SYSTEM II (CESAS II)," *U.S. Marine Corps Concepts & Programs*, http://www.candp.marines.mil/Programs/Focus-Area-4-Modernization-Technology/Part-2-Information-Operations/Part-22-ISR/CESAS-II/.

[27] MCWP 3-40.5; MAGTF Electronic Warfare Capabilities; RadBn Electronic attack equipment; 5-3. MEWSS is funded through USMC Intelligence/Electronic Warfare Systems (MIP) Program Element 0206625M. Funding for MEWSS was last requested in FY2010.

[28] IHS Jane's, "Mobile Electronic Warfare Support System MEWSS)," *C4ISR & MIssion Systems: Joint & Common Equipment*, July 5, 2005, at https://janes.ihs.com/Janes/Display/jmc_4688-jc4ij.

[29] "MEWSS: Electronic warfare vehicle," *Military Today* (2019), at http://www.military-today.com/apc/mewss.htm.

Figure 10. Mobile Electronic Warfare Support System

Source: http://www.military-today.com/apc/mewss.htm.

EW in the Current Strategic Environment

During the Cold War, competition in EW capabilities was an ongoing and significant component of the overall competition in military capabilities between the U.S.-led NATO alliance and the Soviet-led Warsaw Pact alliance. The end of the Cold War and the shift in the early 1990s to the post-Cold War era—a period that featured reduced tensions between major powers and a strong U.S. military emphasis on countering terrorist and insurgent organizations—may have led to a reduced emphasis in U.S. defense plans and programs involving EW related to so-called high-end warfare, meaning high-intensity warfare against technologically sophisticated adversaries.[30]

The perceived shift in the international security environment from the post-Cold War era to an era of renewed great power competition has led to a renewed focus on EW in U.S. defense planning and programming.[31] In particular, U.S. defense planning has focused on aspects of EW related to high-end warfare, and to concerns among some observers that the United States needs to strengthen its EW capabilities as part of its overall effort to preserve U.S. qualitative military superiority over potential adversaries such as Russia and China.

China and Russia have developed sophisticated anti-access/area denial (A2/AD) systems to deny U.S. military forces many advantages; Chinese and Russian EW systems are considered A2/AD systems that deny the U.S military access to their communication and command and control. DOD notes that Russia has emphasized EW in its military modernization effort.[32] Russia reportedly has employed EW as part of its military operations in Ukraine and Syria.[33] DOD

[30] Department of Defense, *National Defense Strategy 2018*.

[31] For more on this shift, see CRS Report R43838, *Renewed Great Power Competition: Implications for Defense—Issues for Congress*, by Ronald O'Rourke.

[32] See Department of Defense, Defense Intelligence Agency, *Russia Military Power, Building a Military to Support Great Power Aspirations*, 2017, pp. 32, 42.

[33] See, for example, Yuri Lapaiev, "Ukraine as Clandestine Testing Ground for Russian Electronic Warfare," *Eurasia Daily Monitor*, vol. 15, issue 157, November 5, 2018; "Russia Deploys Electronic Warfare in Syria," *Army*

similarly states that China recognizes the importance of EW in modern military operations and is developing its EW capabilities as an integral part of its broad-based military modernization effort.[34] China encouraged greater integration between its civil and military technological and industrial bases,[35] which may enable its EW capabilities to benefit from the sophistication of its extensive civilian electronics industry.[36]

Overview of Russian EW Capabilities and Operations

For more than a decade, the Russian military has focused on modernizing its forces, with a particular emphasis on command, control, communications, and computers (C4) and intelligence, surveillance, and reconnaissance (ISR) systems, of which EW plays an important part. According to military analyst Robert McDermott, the Russian military views electronic warfare as a "type of armed struggle using electronic means against enemy C4ISR to 'change the quality of information,' or using electronic means against various assets to change the condition of the operational environment."[37] McDermott describes a close relationship between Russian signals intelligence forces and EW forces, where several EW units perform signals intelligence (SIGINT) functions—similar to U.S. ground force organizations such as the Marine Corps' Radio Battalions. What distinguishes Russian EW organizations, he claims, is also a close relationship with air defense and artillery.[38]

According to the Defense Intelligence Agency (DIA), the Russian military first tested its military modernization efforts in the Georgian war in 2008. DIA notes that "Russian military limitations were fully on display during the August 2008 "five-day war" with Georgia. Russian forces prevailed and defeated their relatively weak Georgian opponents, but after-action analysis by the Russian military highlighted many failings."[39] Based on this operational experience, Russian forces began instituting what is termed the "New Look Program."[40] According to the DIA,

Recognition, October 17, 2018; "New Russian Electronic Warfare Systems Identified in Donbas," *Ukrinform*, September 11, 2018; Jonas Kjellén, *Russian Electronic Warfare, The Role of Electronic Warfare in the Russian Armed Forces*, Swedish Defence Research Agency (FOI), September 2018, 105 pp.; "Russia Tests Electronic Warfare Tools on U.S. Troops in Syria," Unian Information Agency, August 1, 2018; Lara Seligman, "Russian Jamming Poses a Growing Threat to U.S. Troops in Syria," *Foreign Policy*, July 30, 2018; Anna Varfolomeeva, "Signaling Strength: Russia's Real Syria Success Is Electronic Warfare Against the US," *Defense Post*, May 1, 2018.

[34] See Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018*, p. 74. For more on China's military modernization effort, see CRS Report R44196, *The Chinese Military: Overview and Issues for Congress*, by Ian E. Rinehart, and CRS Report RL33153, *China Naval Modernization: Implications for U.S. Navy Capabilities—Background and Issues for Congress*, by Ronald O'Rourke.

[35] For more on these efforts, see Department of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018*, pp. 1-2, 81, 84-85, 121.

[36] For an example of these types of activities, see CRS In Focus IF10119, *U.S.-China Relations*, by Susan V. Lawrence, Michael F. Martin, and Andres B. Schwarzenberg.

[37] Robert N. McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 3, International Centre for Defence and Security, September 2017. See Department of Defense, Defense Intelligence Agency, *Russia Military Power, Building a Military to Support Great Power Aspirations*, 2017, p. 42.

[38] Robert N. McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 5, International Centre for Defence and Security, September 2017.

[39] Department of Defense, Defense Intelligence Agency, *Russia Military Power, Building a Military to Support Great Power Aspirations*, 2017, p. 12.

[40] Department of Defense, Defense Intelligence Agency, *Russia Military Power, Building a Military to Support Great Power Aspirations*, 2017, p. 12.

> [p]artially-manned Soviet-style divisions were reorganized into what were planned to be fully-manned brigades; officer ranks were trimmed from 350,000 billets to initially 150,000, although later the number rose to 220,000; the contract manning effort was reshaped and reinvigorated, with a goal of 425,000 professional enlisted personnel in the force by 2017; the six extant military districts were reshaped initially into four joint strategic commands, which controlled all military assets in their areas in peace and war; and lastly, a massive state armaments program was initiated, allocating 1.1 trillion rubles over 10 years, aiming at fielding a Russian military with 70% new or modernized equipment by 2020.[41]

Investments in EW, through the New Look Program, have been significant. Since 2008, Russian military forces have continued to transform EW capabilities and organizations.

> There are some clues in the many statements by the defence ministry and senior EW officers that indicate the modernisation of EW is based on examining how such capability has been exploited by the US and NATO in military operations over the past two decades. There also appears to be some influence based on US Prompt Global Strike and developments in US and NATO high-precision weapons that is pushing the defence ministry to plan for countering these. At the outset, despite the opaque nature of the overall aims of the procurement processes, one statement that stands out is from the leadership of KRET, aware of the underlying drivers behind the need for modern EW systems in Russia's military.
>
> Indeed, by November 2016, the First Deputy General Director of KRET, Vladimir Mikheyev, referred to the "National Strategic EW System" as an "asymmetric response to the network centric system of combat operations" on the *Murmansk*-BN as a key part of the subsystem.[42] The *Murmansk*-BN has a reported range of 5,000 km, is deployed on seven trucks, and monitors activity on airwaves, intercepting enemy signals with a broad jamming capability; it uses 32-metre-high antennas and has been deployed in Crimea. Mikheyev said the creation of the Russian EW strategic system can be called the "implementation of a network centric defence concept".[43]

Additionally, Russian forces have begun introducing EW forces into their main combat arms organizations. Both McDermott and the DIA indicate that each motorized brigade has at least one electronic warfare company—numbering more than 100 personnel—to provide desired tactical effects (as depicted in **Figure 11**). **Appendix A** provides an overview of the organization and types of equipment these EW companies use.

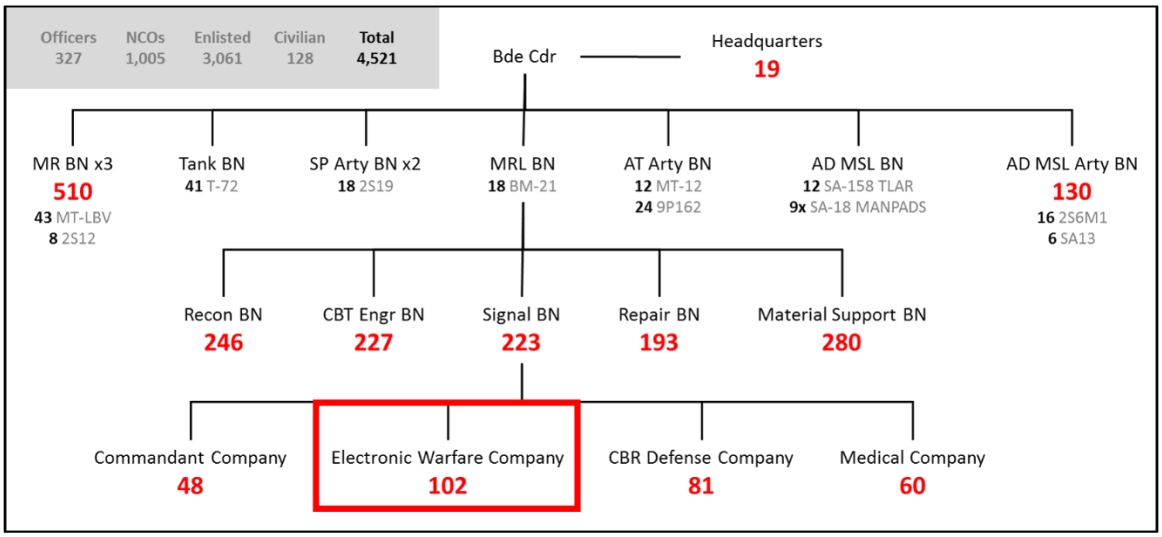
[41] Department of Defense, Defense Intelligence Agency, *Russia Military Power, Building a Military to Support Great Power Aspirations*, 2017, p. 12.

[42] According to IHS Janes the Murmansk-BN is a long-range EW system designed to detect and jam high frequency communications.

[43] Robert N. McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 15. International Centre for Defence and Security, September 2017.

Figure 11. New Look Motorized Rifle Brigade Table of Organization and Equipment

Primary and Supporting Subunits



Source: Department of Defense, Defense Intelligence Agency, *Russia Military Power, Building a Military to Support Great Power Aspirations*, 2017, p. 53.

Overview of Chinese EW Capabilities

China has also seen a similar progression in EW capabilities over the past decade. Most defense analysts focus on Chinese aviation, maritime, and anti-space capabilities; however, the People's Liberation Army (PLA) has developed highly capable systems in the ground domain. China has developed a concept of "informationized warfare," which attempts to gain an advantage in information through robust ISR networks, while attempting to deny adversaries access to information—thus preventing them the ability to command and control forces.[44] To accomplish this goal, the PLA organizes EW functions in a new command called the Strategic Support Force, which includes cyber, psychological, information, and space forces.[45]

Most of the focus on Chinese EW operations has been on air, maritime, and the space domains. However, China has developed sophisticated capabilities to counter U.S. forces on the ground as well. According to Jane's Defence Weekly, China has invested substantial resources into science and technology initiatives focused on improving its network and electronic warfare capabilities.[46] These investments include ground-based sensors and jammers, space-based intelligence assets, and a number of airborne jammers.[47] China has also invested in many unmanned systems that can

[44] Tate Nurkin, Kelly Bedard, James Clad, et al., *China's Advanced Weapons Systems*, IHS Jane's, May 12, 2018, https://www.uscc.gov/sites/default/files/Research/Jane%27s%20by%20IHS%20Markit_China%27s%20Advanced%20Weapons%20Systems.pdf, and Jeffery Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, RAND Corporation, Santa Monica, CA, February 1, 2018, https://www.rand.org/pubs/research_reports/RR1708.html.

[45] Department of Defense, Defense Intelligence Agency, *China Military Power: Modernizing a Force to Fight and Win*, 2019, p. 42.

[46] Tate Nurkin, Kelly Bedard, James Clad, et al., *China's Advanced Weapons Systems*, IHS Jane's, May 12, 2018, p. 11, https://www.uscc.gov/sites/default/files/Research/Jane%27s%20by%20IHS%20Markit_China%27s%20Advanced%20Weapons%20Systems.pdf.

[47] Elsa Kania, *China's Strategic Situational Awareness Capabilities*, Center for Strategic and International Studies,

swarm to provide desired effects, including signals intelligence interceptions and electronic attack.[48]

Potential Issues for Congress

- **Balance of Ground EW Capabilities.** A potential oversight issue for Congress is the balance of EW capabilities the Army and Marine Corps are fielding and plan to procure. During the height of the conflicts in Iraq and Afghanistan, EW programming was weighted toward counter-IED programs rather than on countering great power competition. Although U.S. military forces continue to operate in high-threat IED areas—as illustrated by recent casualties in Afghanistan—these programs do not necessarily provide the necessary protection against potential Russian or Chinese weapons systems. [49] Both services have acknowledged that they require new investments to support command and control in an electromagnetically contested environment.[50] Congress may review how both the Marine Corps and Army allocate resources to counter the IED threat, while working to ensure that ground services are prepared to counter emerging threats.

  Part of the capabilities balance is overlapping programs between the Army and Marine Corps. As both the Army and Marine Corps have EW programs with similar functions. For instance, both services are developing competing C-UAS programs—the Army MEHL and the Marine Corps CLaWS—that appear to have similar capabilities. C-IED programs, on the other hand, are joint programs in which one service develops a solution that other services can procure (thus all DOD services use the same programs which can have efficiencies for sustainment). Congress may examine if it is worthwhile for the Army and Marine Corps to develop competing programs, or if funding competing programs allows technology research and development (R&D) to make greater progress.
- **Funding of Programs.**[51] Funding for EW systems can be difficult to track due to the complexity and classification of EW programs.[52] One challenge associated with ground EW funding is that both the Army and the Marine Corps use research and development appropriations to potentially fund procurement activities due to the relatively fast-paced changes to electronic components. A second, but related, challenge is tracking EW programs when they transition from

Washington, DC, July 29, 2019, https://ontheradar.csis.org/issue-briefs/china-situational-awareness/.

[48] Tate Nurkin, Kelly Bedard, James Clad, et al., *China's Advanced Weapons Systems*, IHS Jane's, May 12, 2018, p. 41, https://www.uscc.gov/sites/default/files/Research/Jane%27s%20by%20IHS%20Markit_China%27s%20Advanced%20Weapons%20Systems.pdf.

[49] See, for example, Department of Defense News Release: *DOD Identifies Marine Casualties*, April 9, 2019, at https://dod.defense.gov/News/News-Releases/News-Release-View/Article/1810150/dod-identifies-marine-casualties/.

[50] Statement of General Robert Neller before the Senate Armed Services Committee [hearing] on Posture of the Department of the Navy, April 9, 2019. Statement of Secretary of the Army Mark Esper and General Mark Milley before the Senate Armed Services Committee [hearing] on Posture of the Department of the Army, March 26, 2019.

[51] For more discussion on EW funding, see CRS Report R45756, *U.S. Military Electronic Warfare Program Funding: Background and Issues for Congress*, by John R. Hoehn.

[52] See Sydney Freedberg Jr., *Breaking Defense* "Electronic Warfare Funding Up, But Short of DSB Marker," accessed May 1, 2019, at https://breakingdefense.com/2018/11/electronic-warfare-funding-up-still-short-of-dsb-recommendation/.

development to procurement. Part of the challenge is that the procurement activities for EW systems can be relatively small compared with larger weapons systems. As a result, DOD procurement activities do not necessarily disclose these components from the larger acquisition, making it difficult to track both a breakout of EW components associated with larger systems (e.g., the M1 Abrams main battle tank) and the total dollar figure associated with EW procurement activities for the Army and Marine Corps.

The Marine Corps and the Army use different funding policies to maintain EW programs. Many of the Army's EW capabilities, as either demonstrators or prototypes, receive R&D funding. As a result, funding for these programs is generally seen as inconsistent and lacking plans for sustainment. The Marine Corps' programs, on the other hand, are programs of record, receiving both R&D and procurement funding.[53] By making these systems programs, the Marine Corps seeks to provide predictable funding for systems over long periods of time. However, these systems are developed through the acquisition system and therefore might not be at the forefront of technological advances.

- **Emerging Technologies.**[54] Emerging technologies may change how the Army and Marine Corps conduct EW. Some experts argue that advances in electronics are already changing how ground forces perform electronic warfare, particularly with continuously improving active electronically scanned arrays and new software defined radios. Some argue that these advances in electronics, paired with artificial intelligence, could allow for some automated decision making.[55] These algorithms could help manage the electromagnetic spectrum by making spectrum allocation decisions, determine when adversaries are jamming (or denying) a frequency band, and automatically develop a jamming plan to deny adversaries access by looking at trends in their electronic emissions. Artificial intelligence algorithms could also enable EW systems to locate and engage small unmanned aerial systems by using data sources to help identify radar contacts (versus environmental clutter from clouds or animals) and electronic emissions. Neither the Army nor the Marine Corps have publicly stated that they plan to use artificial intelligence for managing electromagnetic spectrum operations or electronic warfare.

  New materials are changing the size, weight, power, and cooling of electronics components and power supplies. Electronics are smaller and require less power, and therefore smaller batteries. These new electronics emit less heat because of their reduced consumption of energy, requiring less cooling to maintain ideal temperatures, further reducing energy consumption. Battery technology is improving energy density. These designs provide similar electrical power outputs while reducing their size and weight, making it easier to develop man-portable electronics (such as the Thor C-IED system and the CESAS II jammer).

[53] According to the Defense Acquisition University, a program of record is defined as program that is funded in the future years defense program or has an approved acquisition program baseline.

[54] For an overview of defense emerging technology issues see CRS In Focus IF11105, *Defense Primer: Emerging Technologies*, by Kelley M. Sayler.

[55] Kelsey D. Atherton, "To understand autonomous weapons, think about electronic warfare," *C4ISR Net*, November 15, 2018, https://www.c4isrnet.com/electronic-warfare/2018/11/15/to-understand-autonomous-weapons-think-about-electronic-warfare/. For more discussion on the implications of Artificial Intelligence see CRS Report R45178, *Artificial Intelligence and National Security*, by Kelley M. Sayler.

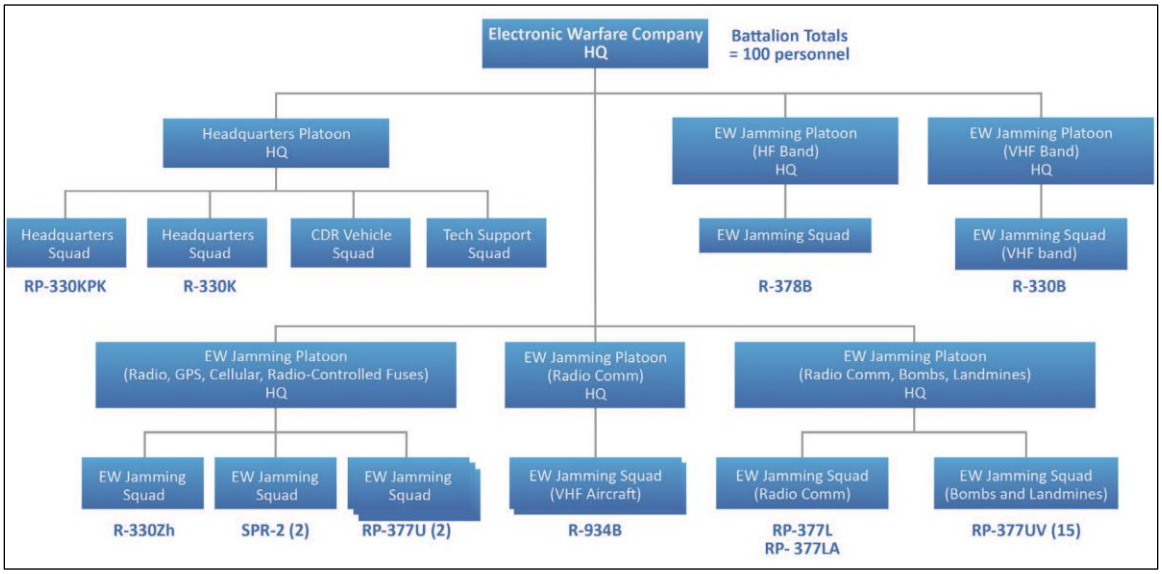
Furthermore, advances in electronics allow for new waveforms using advanced electronically scanned array (AESA) antennas and other designs. As new materials emerge, DOD may request additional funding to upgrade EW systems and potentially procure AESA technology to more effectively jam enemy communications and radar systems.

Quantum technologies could potentially change electronic warfare. Emerging developments in quantum communications and quantum radars will likely change how the military communicates and observes enemies.[56] Quantum technologies will likely have an impact on EW; however, the exact impact they will have on executing EW operations remains unclear.

[56] For more discussion on the use of quantum radars see John Haystead, "Quantum Radar Sees the Light," *Journal of Electronic Defense*, July 2019, pp. 23-31.

Appendix A. Russian EW Company Equipment

Figure A-1. Key EW Equipment



Source: Robert N. McDermott, *Russia's Electronic Warfare Capabilities to 2025*, p. 7. International Centre for Defence and Security, September 2017.

Notes: RP-330KPK: VHF Automated Command Post; RP-330K: Automated Control Station; R-378B: HF Automated Jamming Station; R330B: VHF Frequency Jammer linked to the Borisoglebsk-2 HF Automated Jamming System; R-330Zh: Zhitel Automated Jammer against INMARSAT and IRIDIUM satellite communication systems, GSM and GPS; SPR-2: VHF/UHF Radio Jammer; RP-377U: Portable Jammer (against IEDs); RP-934B: VHF Automated Jamming Station against communications and tactical air guidance systems; RP-377L: IED Jammer; RP-377LP: Portable Automated Jammer; RP-377UV: Portable Automated Jammer.

Author Information

John R. Hoehn
Analyst in Military Capabilities and Programs

Acknowledgments

This report benefited from research efforts by Peter Leutz during his internship with the Congressional Research Service.

Disclaimer