New Weapons, New Options: Electronic Attack in Multi-Domain Operations

A Monograph

by

MAJ Evan E. Roderick
US Army

School of Advanced Military Studies
US Army Command and General Staff College
Fort Leavenworth, KS

2021

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
23 05 2019	MASTER'S THESIS	JUNE 18-MAY 19

4. TITLE AND SUBTITLE
New Weapons, New Options: Electronic Attack in Multi-Domain Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
MAJ Evan E. Roderick

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, KS 66027-2301

8. PERFORMING ORG REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
ADVANCED MILITARY STUDIES PROGRAM

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for Public Release; Distribution is Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Modern militaries rely upon the electromagnetic spectrum to operate. Therefore, attacking electronics and information systems through jamming and directed energy degrades a modern adversary's warfighting system. After the Cold War, America's adversaries invested in electronic attack capability while the US Army largely divested its own. Aware of this, the Army is now investing in old and new electronic weapons to close the gap, regaining electronic attack capability as the Army experiments with the Multi-Domain Operations concept. The purpose of this monograph is to answer the question, "How may the US Army leverage electronic attack in the MDO space?" This monograph proposes that operational land forces should integrate emerging jamming and directed energy weapons into a warfighting system that converges physical, cybernetic, and moral effects upon the enemy in depth. This proposal has significant implications for doctrine, organization, and leader development. The author's intent is to encourage Army leaders to consider offensive actions in the EMS as essential to combined arms operations on the current and future battlefield.

15. SUBJECT TERMS
Electronic Warfare, EW, Electronic Attack, EA, Multi-Domain Operations, MDO, Directed Energy, DE, High Energy Laser, Jamming, Electromagnetic Spectrum, EMS, Microwave, AirLand Battle, Russian EW

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. PHONE NUMBER** *(include area code)*
(U)	(U)	(U)	(U)	47	913 758-3300

Monograph Approval Page

Name of Candidate: MAJ Evan E. Roderick

Monograph Title: New Weapons, New Options: Electronic Attack in Multi-Domain Operations

Approved by:

____//signed/1 April 2021/JKG//_____, Monograph Director
James K. Greer, PhD

____//signed/2 APR 2021/MJY//_____, Seminar Leader
Matthew J. Yandura, COL

____//signed/11 May 21/BAP_____, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 20th day of May 2021 by:

_____, Assistant Dean of Academics for Degree Programs and Research, CGSC
Dale F. Spurlin, PhD

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the US Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

Fair use determination or copyright permission has been obtained for the inclusion of pictures, maps, graphics, and any other works incorporated into this manuscript. A work of the US government is not subject to copyright, however further publication or sale of copyrighted images is not permissible.

Abstract

New Weapons, New Options: Electronic Attack in Multi-Domain Operations, by MAJ Evan E. Roderick, 54 pages.

Modern militaries rely upon the electromagnetic spectrum to operate. Therefore, attacking electronics and information systems through jamming and directed energy degrades a modern adversary's warfighting system. After the Cold War, America's adversaries invested in electronic attack capability while the US Army largely divested its own. Aware of this, the Army is now investing in old and new electronic weapons to close the gap, regaining electronic attack capability as the Army experiments with the Multi-Domain Operations concept. The purpose of this monograph is to answer the question, "How may the US Army leverage electronic attack in the MDO space?" This monograph proposes that operational land forces should integrate emerging jamming and directed energy weapons into a warfighting system that converges physical, cybernetic, and moral effects upon the enemy in depth. This proposal has significant implications for doctrine, organization, and leader development. The author's intent is to encourage Army leaders to consider offensive actions in the EMS as essential to combined arms operations on the current and future battlefield.

Contents

Acknowledgements

I would like to thank my wife and son for tolerating my absence while researching and writing this year. Thank you, COL(P) Chuck Lombardo, the Broncos, the Panthers, and every rotational unit (including my own) that jammed their own nets, for helping me see and understand our electronic warfare problem. And thank you Seminar 3 for listening as I beat my drum about it.

Abbreviations

ACR	Armored Cavalry Regiment
ATP	Army Techniques Publication
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance.
CEWI	Combat Electronic Warfare-Intelligence
DE	Directed Energy
EA	Electronic Attack
ES	Electronic Support
EM	Electromagnetic
EMP	Electromagnetic Pulse
EMS	Electromagnetic Spectrum
EP	Electronic Protection
FLOT	Forward Line of Own Troops
FM	Field Manual
GPS	Global Positioning System
HE	High Energy [laser]
HPM	High Power Microwave
IADS	Integrated Air Defense System
IED	Improvised Explosive Device
IEW	Intelligence and Electronic Warfare
JP	Joint Publication
MDO	Multi-Domain Operations
NATO	North Atlantic Treaty Organization
TRADOC	Training and Doctrine Command (US Army)

Figures

Introduction

Electronic warfare (EW) is "the use of electromagnetic energy and directed energy to control the electromagnetic spectrum (EMS) or attack the enemy."[1] At the end of the Cold War, the US Army largely divested itself of the ability to attack the enemy in the EMS. Meanwhile, Russia and China invested heavily in systems designed to degrade and defeat US and NATO network capabilities through the means of electronic warfare. Russia has made EW central to its approach to cripple NATO's command and control architecture, deny Joint fires and effects, and enable its own ground forces to maneuver. China's concept of "Systems Destruction Warfare" is designed for the same. Faced with these threats, the Army has begun exploring new methods of protecting the force and attacking the enemy in the EMS. New technologies, particularly in the realm of directed energy (DE), demonstrate promising results, but it remains to be seen how these weapons will be integrated as part of a larger warfighting system. With the Multi-Domain Operations (MDO) concept still maturing, the Army has an opportunity to frame how it will use emerging land-based electronic attack (EA) capabilities to conduct operational maneuver as part of the Joint Force.

The purpose of this monograph is to answer the question, "How may the US Army leverage electronic attack in the MDO space?" This monograph proposes that operational land forces should integrate emerging jamming and directed energy weapons into a warfighting system that converges physical, cybernetic, and moral effects upon the enemy in depth.[2] The author's intent is to encourage Army leaders to consider offensive actions in the EMS as essential to

[1] US Department of Defense, Joint Staff, Joint Publication (JP) 3-13.1, *Electronic Warfare* (Washington, DC: Government Printing Office, 2012), I-4.

[2] In an effort to inform current All-Domain concepts and doctrine, this monograph will only discuss electronic attack and directed energy weapons systems that could conceivably be fielded before the year 2030. To keep this monograph scoped to within this decade, and to avoid any classification violations, the author limited his source material for EA and DE technologies to open-source news articles and defense industry reports on recent tests of new systems.

combined arms operations on the current and future battlefield.

The literature review will identify the basic principles of electronic warfare, describe the challenges faced by the Joint Force and the Army in the EMS, and provide an overview of service EA doctrine. An examination of two case studies in electronic attack - US Army electronic warfare concepts in *AirLand Battle* and current Russian electronic warfare operations- follows. The research then analyzes the case studies using John Boyd's *Patterns of Conflict* and James Schneider's *Theoretical Paper no. 3: The Theory of Operational Art*. From this analysis, the author will consider how emerging EA and DE capabilities may be integrated by the Army into a cross-domain warfighting system. Concluding the monograph are recommendations to the force.

Literature Review

Basics of Electronic Warfare

TP 525-3.1: The US Army in Multi-Domain Operations states that the Joint Force must compete in the five domains of Air, Land, Sea, Space, and Cyber, as well as the Information Environment and EMS.[3] While forces may conduct operations exclusively in any of the five domains, all modern operations include activity in the electromagnetic spectrum. The EMS is a conceptual construct representing the range of frequencies of electromagnetic radiation. It is part of the physical environment and its use is constrained by physics, technology, and policies that dictate the use of frequency bands.[4] US Army and Air Force doctrines provide effective summaries of the EMS and the capabilities that rely upon it.

Electronic attack was born during the Russo-Japanese War when a radioman discovered that he could deny- or "jam"- Japanese naval vessels from using wireless communications by

[3] US Department of the Army, Training and Doctrine Command (TRADOC) Pamphlet (TP) 525-3-1, *The US Army in Multi-Domain Operations 2028* (Washington, DC: Government Publishing Office, 2018).

[4] US Department of the Air Force, Air Force (AF) Annex 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations* (Washington, DC: Government Publishing Office, 2019), 5-6.

transmitting noise on the ships' frequency.[5] The activities of detecting, protecting, and attacking within the EMS characterize the three divisions of electronic warfare: Electronic Warfare Support (ES), Electronic Protection (EP), and Electronic Attack (EA).[6] Electronic warfare support consists of the actions taken to identify electromagnetic (EM) energy emitted by the enemy in order to build the threat order of battle and facilitate targeting. Electronic protection represents the hardware, tactics, and techniques employed by friendly forces to protect systems from the effects of both friendly and enemy electronic attack. EA is "the use of electromagnetic (EM) energy, directed energy (DE), or antiradiation weapons to attack personnel, facilities, or equipment."[7] Mario de Archangelis and Alfred Price published excellent histories on the development of EW in 20th century militaries.[8]

EA is used both in the offense and the defense and includes EM jamming, positioning, navigation and timing (PNT) denial, EM deception, DE, antiradiation missiles, and active decoys. EM jamming consists of projecting signals on the same band(s) of frequency used by an adversary's system to deny, disrupt, or deceive it. Jamming represented the bulk of the electronic attack capability development during the 20th century. DE weapons focus high amounts of electromagnetic energy and include lasers, high powered microwave (HPM) emitters, and electromagnetic pulse (EMP) weapons. DE is distinct from the other forms of electronic attack in that, while jamming radiates energy to cause degrading or deceptive effects in the EMS, DE weapons concentrate energy directly upon enemy electrical components and systems in order to deny, degrade, or destroy them. Moreover, the direct and collateral effects of a DE attack can have lethal effects, whereas the other forms of EA typically do not. Anil Maini's *Handbook of*

---

[5] Mario Arcangelis, *Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts* (Blandford Press: Dorset, United Kingdom, 1985), 11-12.

[6] US Joint Staff, JP 3-13.1, I-4

[7] Ibid., I-4 - I-6.

[8] Arcangelis, *Electronic Warfare*; Alfred Price, *War in the Fourth Dimension: US Electronic Warfare from the Vietnam War to the Present* (London: Greenhill Books, 2001).

Defence Electronics and Optonics, published in 2018, is a comprehensive textbook describing the technology and physical principles of electronic warfare and directed energy systems.[9]

The US Military's Electronic Warfare Challenge

Modern militaries network sophisticated electronics, sensors, and computers together to facilitate the rapid detection and destruction of their enemies. The effectiveness of this system in the first Gulf War, combined with force reduction mandates, convinced US military leaders to redesign the force around networked capabilities. This decision paralleled similar developments across all sectors of society, linking humans with machines through increasingly efficient (and often automated) electronic networks. Described by Norbert Wiener's theory of "cybernetics," this increasing interconnectivity corresponded with an increasing vulnerability in the EMS.[10] While the US and its adversaries increased their reliance upon a free EMS for both civil and military infrastructure, the US Army failed to steward its offensive EW capability following the Cold War.[11]

As we doubled-down on network-centric warfare, America's adversaries sought the means to exploit our reliance on the EMS. China's long-term strategy to offset the United States' military advantage includes "systems destruction warfare"- a line of effort dedicated to crippling US operational systems. Part of this effort includes electronic attack capabilities that can threaten every type of US system and data link.[12] Viewing it as an inexpensive and effective way to

---

[9] Anil K. Maini, *Handbook of Defence Electronics and Optronics* (Hoboken, NJ: John Wiley & Sons, 2018).

[10] Norbert Wiener, *The Human Use of Human Beings: Cybernetics and Society*, Da Capo Series in Science (1954; repr., Boston: De Capo Series in Science, 1998).

[11] Kenneth King T., "Electronic Warfare and Organizational Encopresis: The Neglect of the US Army and Its Intelligence Branch to Advocate for Warfighting Capabilities in the Electromagnetic Spectrum," (Masters Monograph, School of Advanced Military Studies, US Army Command and General Staff College, Ft. Leavenworth, KS, 2019). King explores why the Army neglected its EW capability in the 1990s and early 2000's, providing context for the Army's current approach toward electronic attack.

[12] Robert O. Work and Greg Grant, *Beating the Americans at their Own Game: An Offset Strategy with Chinese Characteristics* (Washington, DC: Center for New American Security, 2019), 7-8, accessed 30 Aug 2020, https://www.cnas.org/publications/reports/beating-the-americans-at-their-own-game.

degrade NATO command and control and precision fires, Russia has fully integrated EA into its operational doctrine. Reports from the ongoing conflict in the Donbas region of Ukraine indicate that the Russians have fielded EW weapons superior to America's. The most cited report in recent studies on Russian EW is Roger McDermott's *Russia's Electronic Warfare Capabilities to 2025*.[13]

While coming to grips with its EW capability gap over the past ten years, the US military's response has largely been reactionary toward adversary capabilities while neglecting its own offensive EW systems. The Department of Defense (DOD) significantly increased spending on EW programs in recent years. But without a coherent strategy for fighting in the EMS, services are using their allocated EW funds to upgrade existing programs or to procure rapid solutions to their own operational challenges. *Winning the Invisible War*, a report published by the Center for Strategic and Budgetary Assessments, provides a good account of the choices and challenges faced by the Department of Defense moving into a new era of electronic warfare.[14]

One factor that complicates the US military's approach to EW is the emergence of directed energy weapons- weapons that are both lethal and non-lethal, non-kinetic but with the potential to destroy- that do not fit neatly into existing programs or concepts.[15] Confined to laboratories for decades, high-energy weapons' transition from science fiction to fact was limited by their size and power requirements. That hurdle is overcome, and militaries are now testing DE

---

[13] 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), accessed 30 Aug 2020, https://icds.ee/wpcontent/uploads/2018/ICDS_Report_Russias_Electronic_ Warfare_to_2025.pdf.

[14] Bryan Clark, Whitney W. McNamara, and Timothy A. Walton, *Winning the Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum* (Washington, DC: Center for Strategic and Budgetary Assessments, 2019), 19, Accessed 30 Aug 2020, https://csbaonline.org/research/ publications /winning-the-invisible-war-gaining-an-enduring-us-advantage-in-the-electromagnetic-spectrum.

[15] US Library of Congress, Congressional Research Service, *Ground Electronic Warfare: Background and Issues for Congress*, by John R. Hoehn, R45919 (2019), 16, accessed 30 Aug 2020, https://fas.org/sgp/crs/weapons/R45919.pdf.

weapon platforms. For certain targets, DE weapons effectively replace direct fire munitions. The potential of DE weapon programs go far beyond EA's traditional role of suppressing enemy radar and communications systems. Websites such as *The Drive* and *C4ISRNET* provide regular coverage of rumored and official DoD developments in DE technology.[16] Air Force LTG (Ret) Henry Obering's article "Directed Energy Weapons are Real…And Disruptive" provides a good synopsis of existing and potential DE technology and their implications.[17]

Coinciding with the emergence of technologies that could reshape our understanding of fighting in the EMS is the introduction of the Army's latest warfighting concept: Multi-Domain Operations. MDO seeks to suggest how the Joint Force competes in the current operational environment (OE), penetrates anti-access and area denial (A2/AD) systems, dis-integrates those systems, exploits the penetration, and then consolidates gains in a return to competition. Central to the MDO concept are multi-domain formations (with EW capabilities) that can conduct cross-domain maneuver and fires to achieve "convergence": the rapid and continuous integration of all-domain capabilities to attack the enemy in "decisive spaces." Explicit in each tenet of MDO is the imperative to employ effects in the EMS during all stages of competition and conflict.[18] As the Joint Force consolidates each service's future warfighting concepts into one "All-Domain" concept, it will need to reconcile the services' different approaches to electronic attack.[19]

Electronic Attack Doctrine

Electronic warfare developed in tandem with air power. EA took center stage in the US

[16] The Drive, accessed 30 Aug 2020, https://www.thedrive.com/the-war-zone; C4ISRNET, accessed 30 Aug 2020, https://www.c4isrnet.com/ electronic-warfare.

[17] Henry Obering III, "Directed Energy Weapons Are Real, and Disruptive," *Prism* 8, no. 3 (October 2019): 39, accessed 30 Aug 2020, https://ndupress.ndu.edu/Journals/PRISM/PRISM-8-3/.

[18] US Army, TP 525-3-1, 16 and 19-20.

[19] At the time of this monograph's publication, efforts were underway to reconcile differences between the services' future warfighting concepts, primarily those of the Air Force (Joint All-Domain Operations, released in October, 2020) and the Army (Multi-Domain Operations, published in 2018), in order to arrive at a single Joint future warfighting concept.

Air Force during the Vietnam War as competition accelerated within a system of aircraft, radar, surface-to-air missiles, jamming, EA countermeasures, and EA counter-countermeasures.[20] *JP 3-13.1* describes the Air Force's EW focus as the sensing, disruption, and destruction of enemy integrated air defense systems (IADS).[21] Air Force *Annex 3-51* states, "EW is waged to secure and maintain freedom of action in the EMS" and describes control of the EMS in the same terms as control of the air: parity, superiority, and supremacy.[22] *Annex 3-51* fails to describe the role of DE weapons in air or cross-domain operations, despite the service's significant investment in both airborne and ground DE weapon systems.[23] While the same document specifically addresses EA in the domains of air, space, and cyber, it does not directly address EA in support of land or sea forces.

The Space Force's capstone publication, published in August of 2020, provides some insight into how the Space Force conceptualizes electronic warfare. The three strategic responsibilities of the Space Force- preserve freedom of action, enable joint lethality and effectiveness, and provide independent options- all require the service to have freedom of action in the EMS.[24] "Space Electromagnetic Warfare" is one of the Force's seven disciplines of spacepower.[25] Spacepower is a coercive force and space forces must employ offensive and defensive non-kinetic fires as part of orbital and electromagnetic warfare.[26] The *Space Capstone Publication* only references DE once, noting the risk of high-power lasers to spacecraft and other

[20] Arcangelis, *Electronic Warfare,* 166-173.

[21] US Joint Staff, JP 3-13.1, II-14.

[22] US Air Force, Annex 3-51, 14-15.

[23] For Example: In 2017, the Air Force developed the "DE Flight Plan" to install high energy lasers on aircraft to counter missile threats, develop a high-power radiofrequency (RF) weapon to attack electronics and communications networks, and field an HPM drone-defeat system to protect airfields. See Obering, 41.

[24] US Department of the Space Force, Space Capstone Publication, *Spacepower: Doctrine for Space Forces* (Washington, DC: Government Publishing Office, 2020), 29.

[25] Ibid., 7.

[26] US Space Force, *Spacepower*, 51.

assets in orbit.

The US Navy considers the EMS as part of the information environment. It integrates electronic warfare with cyberspace, space, and intelligence as part of its *information warfare* concept to degrade an enemy's access to the information environment and maintain friendly freedom of action in the same.[27] The Navy possesses EA capability on both ships and aircraft. Navy EA-6B Prowlers and EA-18G Growlers use EA for protection and to suppress enemy air defense systems. Shipboard EA systems are used primarily in a protection role against anti-ship missiles and aircraft. When allocated, Navy airborne EA will support Marine and Joint land operations with jamming capability.[28]

The United States Marine Corps (USMC) expounds a combined arms approach to electronic warfare in their doctrine. The USMC "employs EW as a part of maneuver warfare with the intent to disrupt the adversary's ability to command and control forces, thereby influencing the adversary's decision cycle."[29] Ground EW capability is "primarily directed against tactical communications systems," and jamming resources should be committed at decisive points against critical systems, rather than used indiscriminately.[30] The Marines are investing in DE weapons to defeat drones, but the implications of this capability are not yet addressed in their doctrine. While *MCRP 3-32D.1* discusses the important role of EA in maneuver, the USMC divested its airborne EA-6B Prowler (and its associated technical EW experts) and focused on defeating improvised explosive devices (IEDs) over the past twenty years. As a result, the Marines have much ground

[27] US Department of the Navy, Naval Doctrine Publication (NDP) 1, *Naval Warfare* (Washington, DC: Government Publishing Office, 2020), 35.

[28] US Joint Staff, JP 3-13.1, II-13.

[29] US Joint Staff, JP 3-13.1, II-12.

[30] US Department of the Navy, United States Marine Corps, Marine Corps Reference Publication (MCRP) 3-32D.1, *Electronic Warfare* (Washington, DC: Government Publishing Office, 2018), 3-6 and 3-9 – 3-10.

to cover before their EA capability matches the intent of their doctrine.[31] This is largely the story of EA in the US Army during the same period.

The Army began investing in EA in the early 1970s to protect its helicopters in Vietnam. In 1980, the Army fielded its first ground-based jammer: the TLQ-17A "Traffic Jam."[32] But by the start of the War on Terror, the Army lacked any meaningful jamming capability. Without an operational need for EA, the Army focused its jamming efforts against IEDs.[33] ES and EA were incorporated into the concept of "Command and Control Warfare," doctrinally coordinated by a unit's fires cell.[34] The Army's current fires manual describes the effects of EA primarily in terms of disruption, suppression, and as an element of "preparation fire."[35] *FM 3-12: Cyberspace and EW Operations*, published in 2017, represents the Army's latest conceptual shift for EW, now subsumed by the Army's Cyber branch.[36] By combining EW with Cyber, leaders hope to establish a professional foundation for warfare in the EMS upon which individual specialties can build technical expertise, and then task organize into multi-domain formations as necessary.[37] *ATP 3-12.3: EW Techniques*, serves as the Army's most comprehensive EW doctrine today. Nevertheless, its section on EA does not include ground-based jamming, and there is no dedicated

[31] Jonathan George, "Marine Corps Electronic Warfare: We'll Figure it Out," *Marine Corps Gazette* 102, no. 10 (October 2018): 16, accessed 14 Sep 2020, https://mca-marines.org/wp-content/uploads/2018/12/MCG-October-2018-sm_0.pdf.

[32] Price, *War in the Fourth Dimension,* 183-184.

[33] King, "Electronic Warfare and Organizational Encopresis," 10-11 and 24-25.

[34] US Department of the Army, Army Field Manual 3-36, *Electronic Warfare in Operations* (Washington, DC: Government Printing Office, 2009), 2-4. This manual is now obsolete.

[35] US Department of the Army, Army Field Manual 3-09, *Field Artillery Operations and Fire Support* (Washington, DC: Government Publishing Office, 2014), p 1-4 – 1-5 and 3-14.

[36] US Department of the Army, Army Field Manual 3-12, *Cyberspace and Electronic Warfare Operations* (Washington, DC: Government Publishing Office, 2017).

[37] Mark Pomerleau, "Here's how the Army is grooming an elite cadre of (electronic) cyber soldiers," *Fifth Domain*, 13 Sep 2018, accessed 16 Sep 2020, https://www.fifthdomain.com/dod/army/2018/09/13/heres- how-the-army-is-grooming-and-elite-cadre-of-electronic-cyber-soldiers/.

section for DE.[38] Like the other services, Army doctrine does not yet address the integration of the EA systems into which it is investing.

Joint Force doctrine states that EA is a form of fires and that EA is used "to gain and maintain friendly advantage within the electromagnetic operational environment and ensure requisite friendly access to the EMS."[39] The manual for the Joint Application of Firepower (JFIRE) dedicates a chapter to EA and recommends both a framework for the application of EA assets as well as recommended jamming authorities for tactical situations.[40] In the realm of DE, *JP 3-13.1* discusses the evolution of "Directed-energy warfare" and suggests its implications to Joint Operations.[41] The JFIRE manual does not discuss DE at any length, nor consider the integration and implications of EMP munitions in Joint fires concepts. Interestingly, *JP 3-09*, the military's capstone fires doctrine published in May 2020 states, "the effects of EA can be *lethal* or nonlethal."[42] As this is the most recently published Joint manual regarding EA, the inclusion of "lethal" in the description of EA suggests that emerging DE weapons are influencing US doctrine.

Three observations can be made regarding EA in US military doctrine. The first is that the Joint Force lacks a unifying conception of EA that might better facilitate the convergence of electronic, cyber, information, and kinetic effects in MDO. The second is that service and Joint doctrine place a premium on controlling the EMS. Jamming and electronic attack activities are to be centrally controlled by higher headquarters, both to manage limited assets and to prevent EM

---

[38] US Department of the Army, Army Techniques Publication (ATP) 3-12.3, *Electronic Warfare Techniques,* (Washington, DC: Government Publishing Office, 2019), 6-5 - 6-6.

[39] US Joint Staff, JP 3-13.1, I-10.

[40] US Department of the Army, Army Techniques Publication 3-09.32, *Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower (JFIRE)* (Washington, DC: Government Publishing Office, 2019). This manual is unclassified but its distribution is limited.

[41] US Joint Staff, JP 3-13.1, I-16 – I-17.

[42] US Department of Defense, Joint Staff, Joint Publication 3-09, *Joint Fire Support* (Washington, DC: Government Publishing Office, 2019), III-12.

fratricide. The third observation is that US doctrine does not account for the employment and implications of destructive electronic attack weapons, specifically directed energy weapons. Now that we have established where our EW doctrine stands, let us examine where it was forty years ago.

Case Studies

Electronic Attack in *AirLand Battle*

Witnessing the lethality of modern weapons systems in the 1973 Yom Kippur War and projecting those lessons onto the Soviet threat in Europe spurred the Army into a doctrinal revolution in the late 1970's and early 1980's. Recognizing that North Atlantic Treaty Organization (NATO) defenders would be required to defeat multiple echelons of Soviet and Warsaw Pact armies, the Army adopted *AirLand Battle*, the Army's operating concept that would last until the late 1990s.[43] Published in 1982, the distinguishing feature of *AirLand Battle* was its operational emphasis on the engagement of follow-on echelons far beyond the front lines on an "extended battlefield." From the beginning, *Air Land Battle's* architects recognized that electronic warfare would play a critical role in modern conflicts. The Army's Training and Doctrine Command (TRADOC) integrated EW into the "Army '86" and "Army of Excellence" division force structures, and Army doctrine in the 1980s codified the role of EA in land operations at echelon. In 1991, Operation Desert Storm would test the effectiveness of *AirLand Battle* EW in combat. While *AirLand Battle* sought to employ EA to achieve operational effects, the Army used it primarily to support tactical actions.

In 1981, GEN Don Starry unveiled *AirLand Battle* in *TRADOC Pamphlet (TP) 525-5. AirLand Battle* stated that successful interdiction of second echelon forces required the integration of electronic warfare with fire support, intelligence, and deception. *TP 525-5* stated

[43] John L. Romjue, *From Active Defense to AirLand Battle: The Development of Army Doctrine 1973-1982* (Fort Monroe, VA: US Army Training and Doctrine Command, 1984), 16-17.

that Corps required the capability to jam within 150km of the forward line of own troops (FLOT) with the goal of disrupting or neutralizing half of an enemy's command and control systems.[44] Though lacking the organic ability to jam second echelon forces, Division commanders were to employ their own EA assets to disrupt and delay close-in forces, thus freeing up interdiction assets to conduct deep attacks.[45] Ensuring that divisions had the capability to see and strike deep drove TRADOC's organizational designs that accompanied *AirLand Battle.*

The "Division 86" force design sought to maximize the potential of emerging technologies and resulted in new tables of organizations and equipment, collectively known as the "Army 86" force.[46] The operational and technical relationship between electronic surveillance and jamming led the Army's intelligence community to describe intelligence and electronic warfare (IEW) as one system. However, the Division 86 concept for division-level operations described jamming as a form of fires and linked jamming decisions and coordination directly to the division's fire support element.[47]

The output of this analysis was a redesigned Combat Electronic Warfare – Intelligence (CEWI) battalion that centralized control of the division's EW assets.[48] The approved unit reference sheet for the CEWI battalion included an electronic warfare company equipped with six vehicle-mounted AN/TLQ-17 "Traffic Jam" paired with six TRQ-32 "Teammates" to create an ES/EA system. Additionally, the division's combat aviation brigade received six EH-60 "Quickfix" jammer helicopters. While not assigned to the CEWI battalion, these airborne

---

[44] US Department of the Army, Training and Doctrine Command Pamphlet (TP) 525-5, *The AirLand Battle and Corps 86* (Washington, DC: Government Printing Office, 1981), 43.

[45] US Army, TP 525-5, 10-11.

[46] John L. Romjue, *A History of Army 86: Volume 1* (Fort Monroe, VA: US Army Training and Doctrine Command, 1983), 17.

[47] US Department of the Army, Combined Arms Combat Developments Activity, Memorandum describing the operational concept for heavy division operations on the 1986 battlefield, 8 Jul 1980, CACDA Files, Combined Arms Research Library, Fort Leavenworth, KS, C-1-2 to C-1-3.

[48] Romjue, *A History of Army 86*, 120.

jammers were to remain under the operational control of the division's central jamming authority in the G2/G3 cell.[49] The CEWI organization survived largely intact into the next iteration of Army force design - the "Army of Excellence." All divisions (except light infantry divisions) and armored cavalry regiments (ACR) were allocated jamming capability.[50] TRADOC doctrine writers now had to describe how to employ EA as part of the *AirLand Battle* concept.

The capstone doctrine for *AirLand Battle* was the 1986 version of *FM 100-5: Operations*.[51] *FM 100-5* lists electronic warfare as one of the major functional areas for the operational and tactical levels of war. The G3 or S3 was responsible for coordinating EW, with his primary effort on offensive EW (jamming). Jammers contributed to combined arms operations by disrupting enemy command and control (C2), denying the enemy the ability to react, reducing the effectiveness of air defense and fire support systems, and disrupting the flow of logistics. Manipulative electronic deception- the projection of false signals and communications on enemy networks - was a key consideration in deception planning.[52] *FM 100-5* affirmed that EA was a primary tool for deep operations and included jamming throughout its chapters on the offense and defense.

The IEW manual supporting *FM 100-5* was *FM 34-1: Intelligence and Electronic Warfare Operations*. This manual described the IEW system in detail, at echelon in time and space, according to *AirLand Battle*, noting that the Air Force would be responsible for jamming

[49] Romjue, *A History of Army 86*, 118.

[50] US Department of the Army, Army Field Manual 101-10-1, *Staff Officers' Field Manual Organizational, Technical, and Logistical Data (Volume 1)* (Washington, DC: Government Printing Office, 1987), Chap 2.

[51] While field manuals underwent multiple revisions in the 1980s, the author has endeavored to reference the latest versions published prior to 1990 in order to reflect the doctrine with which units trained and deployed for Operation Desert Storm. The 1986 *FM 100-5* was not updated until 1992 and was the guiding reference for all other IEW and EA manuals discussed in this case study.

[52] US Department of the Army, Army Field Manual 100-5, *Operations* (Washington, DC: Government Printing Office, 1986), 53-54.

second echelon forces and beyond.[53] Chapter 5 was dedicated to offensive EW, known as "electronic countermeasures," consisting of jamming and electronic deception. One principle of EW emphasized the essential integration of EA with fire and maneuver, dictating that jamming resources were to be placed forward and never held in reserve. The manual's recommended priorities for EA were enemy ES and EA systems, surface fire systems, air defense, with enemy C3 links listed last.[54] *FM 34-1* was accompanied by additional manuals describing the IEW system at echelon to assist commanders in employing their jamming assets. While *FM 34-80: Brigade and Battalion IEW* dealt primarily with jamming in defensive operations, *FM 34-35*'s chapters on IEW support to armored cavalry regiments served as the template for mobile jamming operations leading up to Operation Desert Storm.[55] It was with this doctrine that the Army's CEWI battalions deployed to the Persian Gulf.

Operation Desert Storm reversed the strategic assumption of AirLand Battle. Instead of a mobile defense in Central Europe, the opening move would be a deliberate attack in the deserts of Iraq and Kuwait. Preparation for the ground attack involved electronic surveillance across the theater, facilitating the rapid neutralization of Iraqi air defense and strategic command and control systems. The ubiquity of ES during the air campaign and the accuracy of Coalition bombing efforts caused the Iraqis to exercise strict emission control, resulting in limited Iraqi signals to jam once land operations began.[56]

Ground-based EA in Desert Storm was constrained to tactical actions in the close fight, denying the enemy the ability to call for fire or otherwise coordinate for support in the face of the

---

[53] US Department of the Army, Army Field Manual 34-1, *Intelligence and Electronic Warfare Operations* (Washington, DC: Government Publishing Office, 1987), 2-44.

[54] US Army, FM 34-1, 5-9 - 5-11.

[55] Patrick Kelly III, "The Electronic Pivot of Maneuver: The Military Intelligence Battalion (Combat Electronic Warfare Intelligence)" (Masters Monograph, School of Advanced Military Studies, US Army Command and General Staff College, Ft. Leavenworth, KS, 1993), 19.

[56] Price, *War in the Fourth Dimension,* 218 and 222.

Coalition attack. Divisions set forth EW guidance in the "fires" section of operations orders, with priorities established to neutralize enemy fires, air defense, and C2. ES served to identify targets in accordance with the priority of fires.[57] CEWI battalions demonstrated varying degrees of proficiency for offensive jamming operations. Organizing its CEWI company into "Collection & Jamming" platoons, 2nd ACR provided a "rolling baseline" for jamming on the VII Corps front using both Traffic Jam HMMWVs and EH-60s to jam all emitting Iraqi communications. Although successful, 2nd ACR had to overcome substantial organizational and material shortfalls to conduct mobile electronic attack operations.[58] On the opposite end of the spectrum was the 533rd MI BN. Arriving in theater too late to train with its new division, the 533rd did not develop TTPs for EA in the offense and spent the bulk of the ground attack trying to keep pace with the maneuver brigades.[59] Although CEWI organizations had limited opportunity to proof the role of EA in *AirLand Battle* during Desert Storm, the operation demonstrated that EA was part of a system of maneuver, not just intelligence and fires.

While *AirLand Battle* doctrine emphasized the operational role of EA to shape second echelon forces and beyond, limitations in resources and technology manifested in tactically oriented EW doctrine for ground forces. Doctrine and practice evolved to focus upon disrupting first echelon forces' ability to mass. Jamming was a means to reduce the tempo of enemy attacks, presenting brigades and battalions with manageable tactical problems. In action, the Army discovered that many leaders and organizations were not prepared to incorporate electronic attack into operations, specifically the offense.

EW in the Army declined after Operation Desert Storm. When the Army transitioned to

---

[57] US Department of the Army, 24th Mechanized Infantry Division Combat Team, *Operation Desert Storm, OPLAN 91-3* (Washington, DC: Government Printing Office, 1992), 6-9.

[58] Daniel Baker, "Deep Attack: A Military Intelligence Task Force in Desert Storm," *Military Intelligence* 17, no. 4 (Oct-Dec 1991): 39-42, accessed 14 Sep 2020, https://www.ikn.army.mil/apps/MIPBW/ MIPB_Issues/MIPB%20Oct%201991.pdf#view=fit.

[59] Price, *War in the Fourth Dimension,* 219.

the modular force structure in 2004, Divisions lost all jamming capability.[60] Although Army doctrine continued to emphasize the EMS as a critical consideration for the operational environment, organizations, training, and leader development failed to provide the means to affect it. Each service pursued its own concept for electronic attack, manifesting in the doctrine we have today. In the meantime, the Russian Federation made combat in the EMS central to its warfighting concepts.

Electronic Attack in Modern Russia

Russian observations during the Cold War led them to the same conclusion as the United States: victory in future conflict will belong to the side that controls the EMS. Soviet doctrine understood EW as part of an integrated system of ES, EA, and destructive fires known as "radioelectronic combat" (REC). The Soviets fielded capabilities to conduct each REC function down to the division level, with mobile ground-based EW assets acting in concert with corps and higher airborne EW systems.[61] Following the Persian Gulf War and the fall of the Soviet Union, Russian officials began to view EA as an inexpensive, yet critical means to determine the outcome of a conflict.[62] Commentary and published writings by Russian military officials, in addition to heavy investments in technology and equipment, demonstrate the recent emphasis on EW in the Russian Federation. This fruit of this emphasis is an asymmetric advantage in EW that the United States is now endeavoring to close. Today, Russian military concepts, organizations, and operations indicate that Russia integrates EW from the theater to tactical level as part of an operational system designed to deny or control information to its adversaries.

Contemporary writings and operations indicate that "information warfare"- the

---

[60] King, "Electronic Warfare and Organizational Encopresis," 23-24.

[61] D.B. Lawrence, "Soviet Radioelectronic Combat," *Air Force Magazine* 65, no. 3 (March 1982), accessed 16 Sep 2020, https://www.airforcemag.com/article/0382radioelectronic/.

[62] Anya Loukianova, "Moscow's Emerging Electronic Warfare Capabilities: A Dangerous Jammer on U.S./NATO-Russian Relations?" (Unpublished policy memo, Georgia Tech Program on Strategic Stability Evaluation, 2016), 5-6, accessed 17 Sep 2020, https://posse.gatech.edu/sites/default/files /pubfiles/Loukianova-Posse_Russian%20EW_final.pdf.

integration of media, economic tools, psychological operations, cyberspace operations, criminal and subversive actors, and EW with conventional and non-conventional military operations – is considered the decisive element of Russian military strategy. Russia views this system-of-systems approach to shaping the EMS and information environment as central to its strategy against NATO, rendering it impotent in the face of Russian aggression.[63] Russian doctrine separates information warfare into "information-psychological", focused on influencing an adversary's armed forces and population, and "information-technology" warfare, used to affect the technical systems and processes used to collect and transmit information.[64] Jamming appears to have application in both. Russian doctrine also makes a distinction between traditional jamming and what it calls "functional attack"- the use of directed energy and cyber-attacks to suppress or destroy enemy electronic systems.[65] As competition transitions to conflict, the focus on information-technology warfare, and the importance of EA as a means, increases.

Strategically, Russia's combined EA and cyber forces will play a decisive role in the opening stages of conflict by jamming wireless media, by denying basic civilian and military internet service, and by targeting critical civil and military electronic infrastructure. This serves to deny information to adversary populations as well as to deny influence on Russian domestic audiences.[66] EW forces will effectively "black out" communications in a theater, creating a window of time in which conventional and non-conventional forces can maneuver to create a new strategic reality on the ground: the *fait acompli*.

At the tactical-operational level, jamming combines with signals intelligence, air defense,

---

[63] Keir Giles, "Handbook of Russian Information Warfare," (Fellowship Monograph, Research Division, NATO Defense College, Rome, Italy, 2016), 6-7.

[64] Ibid., 9-10.

[65] Jonas Kjellen, *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces* (Stockholm, Sweden: Swedish Defence Research Agency (FOI)), 22, accessed 16 Sep 2020, https://www.foi.se/en/foi/reports.html.

[66] Giles, "Handbook of Russian Information Warfare," 66-67.

and artillery to deny adversary tactical communications, EW, counter-fire radar, and air superiority.[67] Russia also views jamming as a critical protection capability, and equips its ground units with systems designed to thwart electronic guidance and fuse systems on incoming munitions. Overall, Russia views EW as a cost-effective way to achieve an asymmetric advantage over net-centric NATO forces.[68]

Russia integrates EA weapons into strategic, theater, and tactical formations of every service. The EW element on the General Staff coordinates the efforts of EW across Russia's military. Russia's "radiotechnical" soldiers also man and monitor its extensive strategic radar network.[69] Within the ground forces there are five EW brigades from which the maneuver brigades draw their EW companies. Army aviation regiments and brigades have airborne jamming detachments, and Russia's strategic air defense and rocket forces have EW companies and battalions.[70]

In terms of equipment, Russia's most noteworthy strategic jamming capability resides in the *Murmansk-BN* system that can allegedly deny the US Air Force the use of its High Frequency Global Communications System network in theater. Ground-based jamming battalions supporting Russia's air force and air defense forces have systems capable of suppressing airborne and space-based radars. The drone-based *Leer-3* functions as a surrogate cell tower, monitoring phone calls and jamming connections as desired.[71] A host of multi-functional EW systems, with the ability to monitor the EMS, jam, and spoof signals, support brigade and battalion tactical groups. Of note

---

[67] McDermott, *Russia's Electronic Warfare Capabilities,* p 4-5.

[68] Keith Crane, Olga Oliker, and Brian Nichiporuk, *Trends in Russia's Armed Forces: An Overview of Budgets and Capabilities* (Santa Monica, California: RAND Corporation, 2019), 65, accessed 30 Aug 2020, https://www.rand.org/pubs/research_reports/RR2573.html.

[69] Charles Bartles, "Role of Radio-Technical Troops in the Russian Armed Forces," *OE Watch* 06, no. 3 (March 2016): 50, accessed 17 Sep 2020, https://community.apan.org/wg/tradoc-g2/fmso/m/oe-watch-past-issues/195441.

[70] Kjellen, *Russian Electronic Warfare,* 34, 36, and 38.

[71] Ibid., 49-51.

are the *Altaets* and *Zhitel* systems, designed to jam drone and aircraft communications.[72] Russia employs EW capability on drones and mixes EW munitions with conventional payloads on rocket artillery. Understanding NATO's reliance on precision navigation, Russia equips each EW company with the capability to detect and jam global positioning system (GPS) signals.[73] Operations in Ukraine would provide ample opportunity for Russia to test its electronic warfare capabilities and concepts.

Following the ousting of Ukraine's Russian-backed President Viktor Yanukovych in February of 2014, numerous separatist movements emerged in the Russian-speaking eastern region of Ukraine known as the Donbass. As Ukrainian forces suppressed these movements, Russia gradually escalated its support of the separatist fighters until it invaded with conventional forces, engaging the Ukrainian army openly near the town of Ilovaisk in August 2014.[74] Operations against Ukraine's conventional army demonstrated how Russia organizes and employs EW. More than any other conflict, operations in the Ukraine informed current Russian EW doctrine.[75]

Donbass served as a laboratory for Russian EW tactics. Russia organized its EW forces into mobile tactical groups, capable of executing all forms of EW, to include some on the move. Outside of Ilovaysk, ES and EA systems operated at distances up to 240 kilometers from the front lines. Roger McDermott, in his authoritative study on Russian EW capabilities, described the role of EW forces at Ilovaysk as: "suppressing radio communications at tactical and operational levels, fixing and locating enemy forces by identifying EMS usage, disrupting C2, blocking

---

[72] Kjellen, *Russian Electronic Warfare,* 44

[73] Charles Bartles, "Recommendations for Intelligence Staffs Concerning Russian New Generation Warfare," *Military Intelligence Professional Bulletin* 43, no. 4 (Oct-Dec 2017): 15, accessed 17 Sep 2020, https://www.ikn.army.mil/apps/MIPBW/MIPB_Issues/ MIPBOct_Dec17finalIKN.pdf#view=fit.

[74] Michael Kofman, et al, *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, California: RAND Corporation, 2017), 33-45, accessed 10 Sep 2020, https://www.rand.org/pubs/research_reports/RR1498.html.

[75] McDermott, *Russia's Electronic Warfare Capabilities,* 21 and 25.

mobile phone networks, and spreading false information as part of psychological operations."[76] Building from its experience in Ilovaysk, the army organized an EW task force specifically to monitor the EMS and develop the electronic order of battle prior to its next direct confrontation with Ukraine in Debaltseve.[77]

In execution, the Russians used a mix of jamming, signal intercept, and direction finding to disrupt, collect, and target Ukrainian forces. Jammers served in an effective counter-reconnaissance role, blocking or spoofing GPS receivers on Ukrainian small UAS platforms. Russian EW teams also hacked UAS feeds, allowing them to identify Ukrainian positions as the drones returned to base.[78]

Operations in eastern Ukraine demonstrated the integration of electronic attack capabilities with other means to create cross-domain systems of attack.[79] In 2015, Russia apparently sabotaged Ukrainian radios by projecting a signal that activated a virus already embedded in the equipment. With their issued radios rendered useless, soldiers turned to commercial radios and cell phones, which the Russians subsequently jammed and used for targeting.[80] Russia also integrates EA into information and psychological operations. EW forces triangulated cell phone signals to facilitate a large rocket artillery attack, which they followed up with text messages asking the defenders if they enjoyed the artillery strike.[81] In Debaltseve,

---

[76] McDermott, *Russia's Electronic Warfare Capabilities,* 26.

[77] Ibid.

[78] Patrick Smith, *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy* (Washington, DC: American Security Project, 2020), 4, accessed 30 Aug 2020, https://www.americansecurity project.org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf.

[79] It is important to note here again that the idea of "domains" is a Western military construct. The Russians do not see EW as residing in any specific warfighting function or physical/cognitive space.

[80] Joseph Trevithick, "Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio "Virus"," The Drive, 30 Oct 2019, accessed 17 Sep 2020, https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus.

[81] US Department of the Army, Asymmetric Warfare Group, *Russian New Generation Warfare Handbook* (Washington, DC: Government Publishing Office, 2016), p 18 and 29-30. This report is "For Official Use Only", but all references here are "Unclassified".

Russia also tested an automated system of jammers paired with ground and drone-based ES sensors.[82]

Russia's conflict in the Donbass both confirmed and informed Russian concepts of electronic warfare. Russia achieved operational and tactical effects through its manipulation of the EMS and the integration of electronic attack with other forms of combat power. The conflict provided a glimpse into the future, showing how militaries can exploit new technologies and combine them with old to wage war in the EMS.

Emerging Electronic Attack Technologies

Drone and Counter-Drone Jamming

UASs and traditional jamming technology have converged to form a new capability. As mentioned in the previous case study, Russia has already installed jammers on drones as part of its *Leer3* EW system. In the United States, the Army and Air Force look to go deeper, testing air-launched, multi-role drone "swarms" that can quickly traverse the battlefield into an adversary's support area to identify, disrupt, and even destroy high-payoff targets. The contract proposal from the Army's Combat Capabilities Development Command requires these drones to be equipped with ES sensors and EA weapons, able to simultaneously detect the enemy order of battle, prosecute jamming, and observe fire missions. The Army's proposal suggests that networked EW drones have a role in the close, deep, and support area. In addition to its integration in the larger collection-fires architecture, EW drone swarms can support operational maneuver through deceptive signals and signatures.[83] While this system has not yet been fielded, the proposal

[82] McDermott, *Russia's Electronic Warfare Capabilities,* 27.

[83] Joseph Trevithick, "The Army Has Unveiled its Plan for Swarms of Electronic Warfare-Enabled Air-Launched Drones," The Drive, 16 Aug 2020, accessed 17 Sep 2020, https://www.thedrive.com/the-war-zone/35726/the-army-has-unveiled-its-plan-for-swarms-of-electronic-warfare-enabled-air-launched-drones; Tyler Rogoway, "SPEAR Mini-Cruise Missile Getting An Electronic Warfare Variant To Swarm With Is A Huge Deal," The Drive, 12 Sep 2019, accessed 17 Sep 2020, https://www.thedrive.com/the-war-zone/29789/spear-mini-cruise-missile-getting-an-electronic-warfare-variant-to-swarm-with-is-a-huge-deal. Both webpages accessed 17 Sep 2020.

indicates that the Army is considering the integration of EA capabilities with its expanding UAS fleet into a broader warfighting system.

Counter-drone jamming systems effectively function as maneuver short-range air defense (SHORAD) weapons, protecting units and critical nodes from observation and attack. Many counter-drone weapons jam or deceive direction-finding and communication systems, causing drones to crash or return home.[84] Ideally, counter-drone EA systems could be linked into a theater's IADS, able to rapidly deconflict airspace and discern friend from foe. However, the reactive nature of engagements against low-flying drones in a contested EMS environment will make deliberate airspace and EMS deconfliction unlikely, particularly for dismounts armed with man-portable variants.

High Energy Lasers

The destructive potential of directed energy weapons is derived from the amount of energy transferred to a target over time. High energy (HE) lasers typically project energy in the kilowatt to megawatt range. On the low end, these weapons can blind sensors. As energy increases, they can degrade sensitive electronic components, heat equipment and personnel to the point that they can no longer perform their functions, and cause fuel or munitions to explode.[85] The US Navy leads the services in implementing HE lasers, installing its first on a surface ship in 2014. It now has a family of lasers on many ships, from optical "dazzlers" to 150 kilowatt beams.[86] Advances in optics, power generation, and propagation methods have made employing HE lasers on sea, in the air and space, and on mobile land systems a reality.

---

[84] John Keller, "Army Asks SRC to Build and Deploy Counter-Drone System to Protect Expeditionary Forces from Enemy UAVs," Military & Aerospace Electronics, 17 Jul 2020, accessed 9 Oct 2020, https://www.militaryaerospace.com/unmanned/article/ 14180310/counterdrone-expeditionary-intelligence-gathering.

[85] Obering, "Directed Energy Weapons Are Real," 38.

[86] Kyle Mizokami, "The Navy Just Tested Its Most Powerful Laser Yet," *Popular Mechanics*, 27 May 2020, accessed 9 Oct 2020, https://www.popularmechanics.com/military/navy-ships/a32676643/navy-laser-weapon-system-demonstrator-test.

Land-based HE laser systems can serve many functions. At the tactical level, HE lasers can protect against incoming munitions, disable drones, and suppress enemy active protection systems as a complement to kinetic fires. The Air Force's truck mounted Recovery of Airbase Denied by Ordnance (RADBO) system uses HE lasers to detonate mines at a comfortable distance.[87] The Army is currently developing a 300kW truck-mounted laser to protect against rockets, artillery, and mortars.[88] At the theater and strategic level, HE lasers might be the only effective counter to hypersonic missiles. Depending on atmospheric conditions and available power, ground based HE lasers could target enemy satellites in orbit.

HE lasers effectively serve as munitions replacements for kinetic weapons. This comes at a cost: power requirements, increased signature in the EMS while engaging, and potential for fratricide due to the long-range and cross-domain effects. HE lasers can also be limited by atmospheric conditions, although advances in the field are working to overcome that challenge.[89]

Non-Lethal, Anti-Personnel Directed Energy

The interaction of lasers with elements in the physical environment allows for non-lethal uses for DE. The US military experimented with "Pain Rays" as part of its Active Denial System (ADS) during the height of counterinsurgency operations in Iraq and Afghanistan. Designed for crowd control, this system transforms electricity into millimeter-length radio waves that heat water in the skin to create an unbearable heat sensation in a matter of seconds. Eleven thousand tests of the ADS resulted in only two injuries.[90] Another application involves using lasers to

[87] Aaron Mehta. "Air Force awards laser-armed RADBO contract to Parsons," C4ISRNET, 25 Sep 2020, accessed 4 Nov 2020, https://www.c4isrnet.com/industry/2020/09/25/air-force-awards-laser-armed-radbo-contract-to-parsons/.

[88] Jared Keller, "The Army is Tripling the Power of One of its Vehicle-mounted Laser Systems," Task & Purpose, 8 May 2020, accessed 4 Nov 2020, https://taskandpurpose.com/ news/army-laser-weapon-power.

[89] Obering, "Directed Energy Weapons Are Real," 44.

[90] Spencer Ackerman, "I Got Blasted by the Pentagon's Pain Ray—Twice," Wired, 12 Mar 2012, accessed 4 Nov 2020, https://www.wired.com/2012/03/pain-ray-shot/.

generate balls of plasma near personnel, and then applying other lasers to induce physical effects- such as phantom voices or unbearable noise- in the surrounding air. The Joint Non-lethal Weapons directorate is on the cusp of fielding laser-induced plasma effect weapons to heat a target's skin, create extremely loud or confusing noises, and project verbal commands.[91]

Non-lethal DE weapons have applications for fixed site security, can be used during security and consolidation operations, and can enhance mobility by keeping crowds off roads. However, the novelty of these weapons can create negative effects in the information environment. GEN Stanley McChrystal ordered the removal of the ADS from Afghanistan within weeks of its deployment as the Taliban convinced people that the US was "microwaving" civilians to inflict cancer and infertility.[92]

High Power Microwave Weapons

High power microwave (HPM) weapons are designed to deny, disrupt, damage, or destroy a target's electronics by overwhelming them with EM energy. HPMs are scalable, the desired effect rendered based upon how much energy the HPM projects. At lower ranges, HPMs surge enough power to "lock-up" a system, denying its use. At higher ranges of power, HPMs destroy integrated circuits. Unlike jammers, HPMs can achieve their effects when target systems are not operating. Countering HPMs requires the hardening of an entire electronic system, as surged energy infiltrates through exposed wires, ports, antennae, and optics.[93] Unlike HE lasers, HPMs are area weapons. Destructive effects are generally rendered at closer ranges, while disruptive effects can be achieved over a greater area at longer distances. As area weapons, HPMs

[91] Todd South, "Pentagon Scientists Are Making Talking Plasma Laser Balls for Use as Non-lethal Weapons," *Military Times*, 19 Jul 2019, accessed 4 Nov 2020, https://www.militarytimes.com/news/your-military/2019/07/19/pentagon-scientists-are-making-talking-plasma-laser-balls-for-use-as-non-lethal-weapons/.

[92] Ackerman, "I Got Blasted by the Pentagon's Pain Ray—Twice."

[93] Eileen M Walling, *High Power Microwaves: Strategic and Operational Implications for Warfare* (Maxwell AFB, AL: Center for Strategy and Technology, Air War College, 2000), 2, accessed 15 Sep 2020, www.airuniversity.af.edu/Portals/10/ CSAT/documents/OP/csat11.pdf.

are especially useful against drone swarms, and the Air Force has already fielded at least one HPM weapon to protect its ground facilities against drone attacks.[94] In 2017, Boeing and the Air Force successfully tested the "counter-electronics high power microwave advanced missile project" (CHAMP), a cruise missile designed to destroy computers and electronics with an onboard HPM.[95] Adapting this technology to UASs or a helicopter-based delivery system presents another vector for long-range HPM attacks.

The HPM weapon with the greatest strategic potential is the non-nuclear electromagnetic pulse (EMP). Once American researchers recognized that nuclear explosions were accompanied by massive surges in EM energy, the US and Soviet Union began research to replicate that effect with non-nuclear munitions. While the CHAMP uses onboard batteries to emit its HPM to achieve local effects, an EMP bomb transfers explosive energy into a magnetic field to create an HPM effect across an operational area. Component technologies have matured to the point where an EMP bomb or missile is feasible.[96] While the DoD has not publicized its EMP research, in 2017 it solicited industry for a "munition-delivered non-kinetic effect" with the capability to "neutralize an adversary's underlying industrial, civil, and communications infrastructure without the destruction of the hardware associated with those systems." The proposal directed that the effect be delivered in a standard Army 155mm projectile.[97] The capabilities required from this proposal point to some sort of artillery delivered EMP weapon. With C2 systems and electro-

---

[94] Joseph Trevithick, "Air Force Set to Deploy Its Counter-Drone "Phaser" Microwave Weapon Overseas," The Drive, 24 Sep 2019, accessed 5 Nov 2020, https://www.thedrive.com/the-war-zone/29992/air-force-set-to-field-test-its-counter-drone-phaser-microwave-weapon-overseas-in-2020.

[95] Kelsey D Atherton, "Making Sense of CHAMP, the Silver Bullet Miracle Missile That Isn't," C4ISRNET, 13 Dec 2017, accessed 6 Nov 2020, https://www.c4isrnet.com/electronic-warfare/2017/12/13/making-sense-of-champ-the-silver-bullet-miracle-missile-that-isnt/.

[96] Maini, *Handbook of Defence Electronics,* p 1041-1043.

[97] US Department of Defense, Office of the Under Secretary of Defense for Acquisition & Sustainment, DoD 2017.1 Small Business Innovation Research (SBIR) Solicitation, 30 Nov 2016, accessed 16 September 2020, https://www.sbir.gov/node/1206543. The DoD regularly solicits the private sector to develop technologies for military application through the US Small Business Administration's SBIR initiative.

optical sensors reliant upon sensitive and vulnerable electronics, the effect of a successful EMP strike against an adversary could be decisive.

Having explored the case studies for EA and the potential of new technologies, we will now examine the theoretical frameworks with which we will analyze them.

Analysis

Theory

James Schneider theorized that three domains existed in combat: physical, cybernetic, and moral.[98] The physical domain is concerned with materiel, logistics, terrain, weather, and other features of the physical environment. The cybernetic domain is where combatants make sense of the environment and direct action to ensure cohesion of organizations and effort. Command, control, and information contribute to cohesion. To clarify, Schneider's *cybernetic* domain should not be confused with today's *cyber* domain: "the interdependent network of information technology infrastructure and resident data" that includes the Internet and associated networks and hardware.[99] The moral domain is "concerned with the disintegration and breakdown of will." Will, measured by morale, is "the engine of all action."[100]

These domains align with the stages in defeat of an adversary: cohesion, disorganization, and disintegration. As a combatant inflicts physical destruction upon an adversary over time, those effects begin to unravel the adversary's ability to maintain cohesion of organization and effort. This disorganization accelerates the rate of defeat as forces become uncertain and fearful, lose faith, and then disintegrate. Schneider acknowledges that elements within a force exhibit varying degrees of disorganization and disintegration during an operation, even before they are

---

[98] James Schneider, *Theoretical Paper No. 3: The Theory of Operational Art* (Fort Leavenworth, KS: US Army Command and General Staff College, 1988), 6-7.

[99] Department of Defense, Joint Staff, Joint Publication 3-12, *Cyberspace Operations* (Washington, DC: Government Publishing Office, 2018), I-1.

[100] Schneider, *Theoretical Paper No. 3,* 7.

subjected to destructive effects.

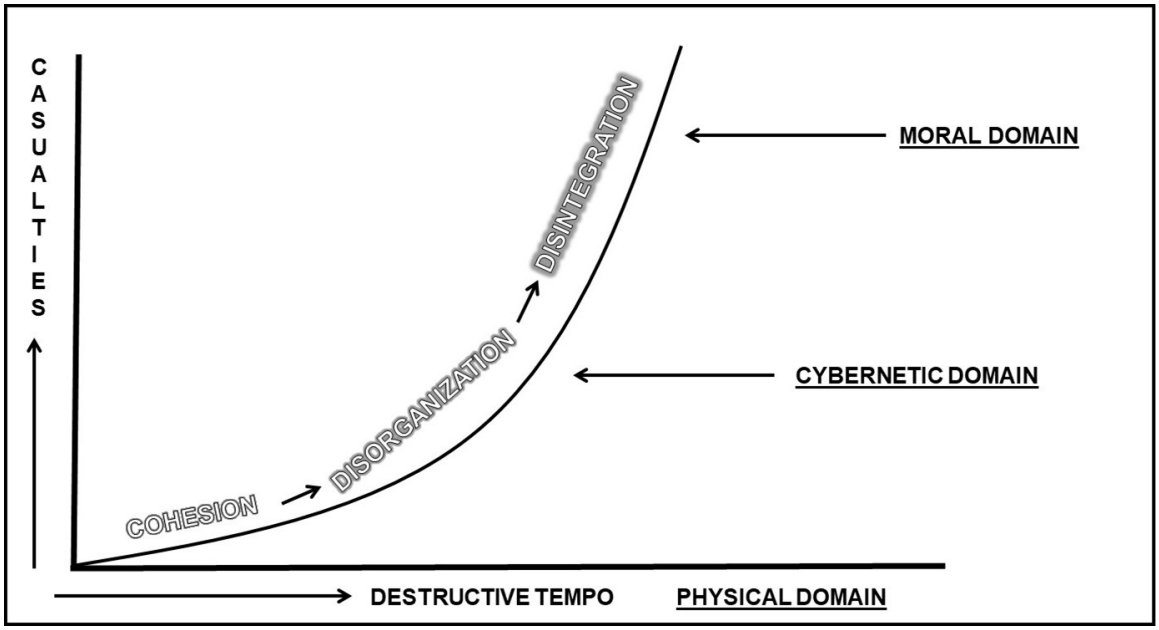

Figure 1. "Destruction, Disorganization, Disintegration." James Schneider, *Theoretical Paper No. 3: The Theory of Operational Art* (Fort Leavenworth, KS: US Army Command and General Staff College, 1988), 5.

Schneider applies his domain framework to his definition of "decisive points." Physical decisive points are geographical. Cybernetic decisive points "sustain command, control, communications, and the processing of information." Moral decisive points sustain an adversary's will to fight. These might include an enemy commander at the tactical level or the political will of key stakeholders at the strategic.[101]

From Schneider's framework, we can deduce that by attacking the enemy's cybernetic and moral decisive points, we will accelerate his destruction and will to resist. This idea is not far from the operational theories of John Boyd.

The military theorist John Boyd is best known for his Observe-Orient-Decide-Act (OODA) cycle. Boyd extrapolated upward from tactical OODA loops to theorize methods of collapsing an adversary's operational and strategic systems.[102] From his study of history, Boyd

[101] Schneider, *Theoretical Paper No. 3,* 28.

[102] John R. Boyd, *A Discourse on Winning and Losing*, ed by Grant T. Hammond (Maxwell AFB, AL: Air University Press, 2018).

asserted that conflicts could be divided into three categories: attrition warfare, maneuver conflict, and moral conflict. He synthesized elements from each to create his own theory of operations.

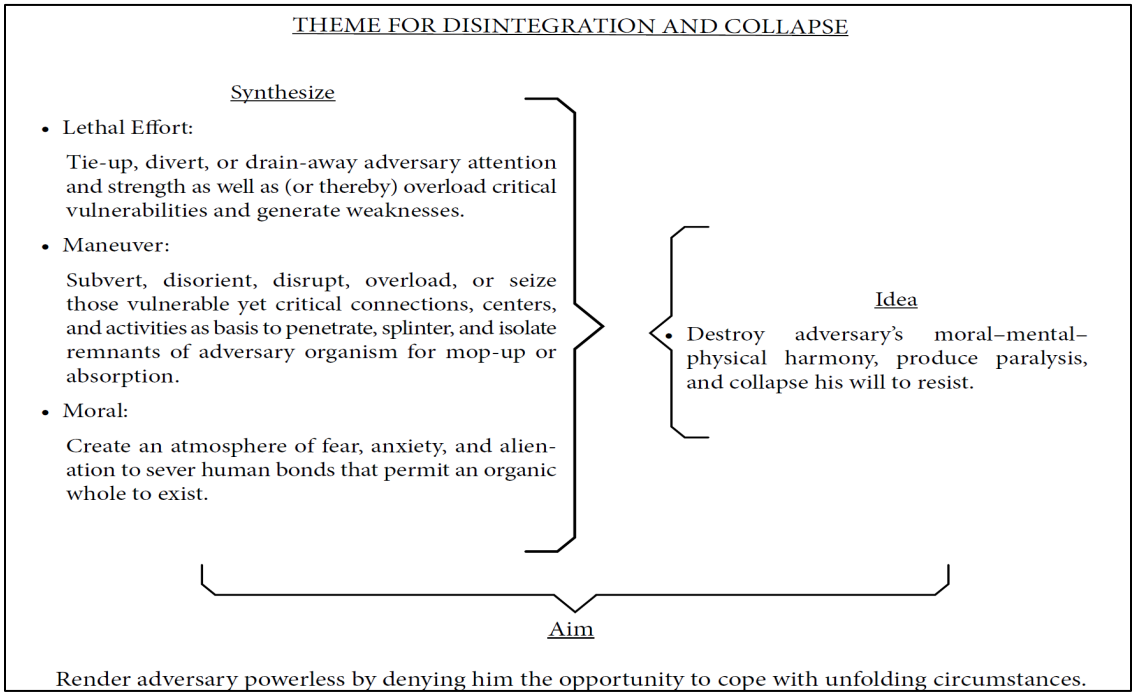

Figure 2. "Theme for Disintegration and Collapse." John R. Boyd, *A Discourse on Winning and Losing*, ed by Grant T. Hammond (Maxwell AFB, AL: Air University Press, 2018), 157.

Lethal efforts represent the actions taken directly against the enemy to reduce his combat power or deny him the use thereof against one's own. Maneuver efforts are indirect approaches taken to disintegrate the enemy system. Moral efforts create menace, uncertainty, and mistrust. An effective synthesis of these efforts results in the disintegration and collapse of an adversary's will to resist.

Analyzing the previous case studies through Schneider and Boyd's frameworks can help us understand the differences and inform the creation of a useful model for the employment of new EA technology on the multidomain battlefield.

Case Study Analysis

Electronic attack in *AirLand Battle* was a tool for attacking the enemy in the cybernetic domain, employed primarily in support of lethal and maneuver efforts. With limited ability to project EA in depth, the Army focused subsequent EA doctrine, training, and operations on the

tactical level.

In *AirLand Battle* doctrine, jamming was an electronic countermeasure tool employed in the cybernetic domain. Jammers deny information, reducing the enemy's ability to provide purpose, direction, and organization toward his aim. The focus for jammers was on the networks that shared information between fires, air defense, and command nodes. These are the cybernetic decisive points in *AirLand Battle*. The other form of EA in *AirLand Battle*, electronic deception, was also oriented on the cybernetic domain.[103] Simulative, manipulative, and imitative signals generated false information into an enemy's calculus, facilitating disorganization by distracting the enemy from his aim.

Boyd considered deception an element of maneuver conflict. In this sense, EA in *AirLand Battle* functioned as part of the maneuver effort. Electronic deception could disorient or subvert information networks and decision-makers, reducing their capacity and time to react to friendly actions. Jamming also functioned in maneuver warfare by "denying the enemy the ability to react to changes on the battlefield" and by disrupting enemy C2, "thus slowing or disorganizing the enemy in critical sections."[104] When massed with fires and other effects, jamming facilitated the penetration of enemy resistance and subsequent destruction or seizure of critical nodes. *AirLand Battle* emphasized the role of maneuver in the defeat of a determined Soviet attack, but much of the doctrine focused on the employment of new capabilities to facilitate lethal effort. EW systems would detect signals, jam them, and facilitate targeting to reduce the adversary's strength. In the first/second echelon paradigm, jamming supported fires to reduce the tempo of the fight and present frontline brigades with more manageable tactical problems.

Army '86 and Army of Excellence EA organizations and equipment were only capable of attacking cybernetic decisive points in the enemy's first echelon.[105] CEWI organizations were

[103] US Army, FM 34-1, 2-17.

[104] US Army, FM 100-5, 54.

[105] US Army, FM 34-1, 2-36, 2-37, and 2-44.

oriented on collection and jamming of tactical formations. This system of detection and attack, oriented on the close fight, primarily facilitated lethal efforts.

Desert Storm demonstrated where Army EA fit within a phased Joint operation to dominate the EMS, setting the conditions for rapid ground maneuver. The opening stage of Operation Desert Storm employed Air Force and Navy-delivered EA effects against cybernetic and moral decisive points as part of both lethal and moral efforts. The net effect of the Coalition's domination of the EMS was a debilitating fear of wireless communication by Iraqi ground units. With little to target, CEWI units maneuvering with their divisions during ground operations maintained a steady jamming baseline to jam the few Iraqis' brave enough to transmit.

While *AirLand Battle* used EA against cybernetic targets as part of maneuver and lethal efforts, Russia employs EA against physical, cybernetic, and moral targets. Russia's integration of EA capabilities into air defense, rocket forces, airborne, and maneuver brigades across its army demonstrate its understanding that EA functions as part of larger lethal and maneuver systems. Operations in the Donbass indicate a growing role for EA in moral warfare.

Like its *AirLand Battle* counterpart, Russian EW doctrine includes electronic countermeasures (jamming) and electronic simulation/imitation (electronic deception) as categories of EA. In addition to these cybernetic effects, the inclusion of functional attack, with its focus on the destruction of enemy systems and platforms with directed energy, indicates that Russia also considers EA as a mechanism for achieving effects in the physical domain. Russian doctrine emphasizes the importance of defeating an adversary's C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) system, consistent with Boyd's maneuver to disorient and disrupt as the basis for penetration and isolation of the adversary. Doctrinal developments in Russia suggest that electronic attack will be combined with cyber operations to target critical civil and military infrastructure.[106] Integrating these attacks in

[106] Kjellen, *Russian Electronic Warfare,* 23.

the moral domain with lethal and maneuver efforts is consistent with Boyd's framework.

Russia's EW force organization reflects its understanding that the EMS must be exploited at every level and stage in conflict to prevail. Russian motorized, tank, airborne, and special purpose forces all have assigned EA capability. Its EA hardware is multipurpose, integrated into a see-strike-protect EW/fires complex that achieves rapid physical and cybernetic effects. The *Leer 3*, used to control cell phone traffic, combined with the *Orlan*-10's ability to send manipulative text messages, represents an EA system employed to conduct moral warfare.

Russia employed EA in the cybernetic and moral domains in the Donbas, but its strategic aims limited EA to attrition and moral warfare. EW forces supported Donbas separatists with targeting information and jamming capability. Russia aimed its EA/fires complex at the will of Ukrainian conventional forces, compelling them into tactical, operational, and strategic recalculation. It is difficult to assess the operational impact of Russia's combined EA-psychological operations against individual Ukrainian Soldiers, but the experience in the Donbas indicates that these moral attacks need to be exploited through maneuver before the victims are immunized to the effect.[107]

Russia views its EW capability as a cost-effective asymmetric advantage over the technology reliant NATO forces. EA weapons also provide Russia with the ability to collapse an enemy's system and will to fight by isolating some units and menacing others, while inflicting just enough casualties to end the conflict and avoid escalation. Russia's aggressive strategy in its near abroad requires capabilities that can rapidly collapse resistance while protecting its own expensive military. EA weapons are critical to this warfighting system.

---

[107] Yuri Lapaiev, "Russian Electronic Warfare in Donbas: Training or Preparation for a Wider Attack?" *Eurasia Daily Monitor* 17, no. 34 (March 2020), accessed 16 Sep 2020, https://jamestown.org/program/ russian-electronic-warfare-in-donbas-training-or-preparation-for-a-wider-attack/.

Implications

Boyd asserts that a combatant must have moral-mental-physical harmony to resist. To destroy this harmony requires combinations of lethal, maneuver, and moral efforts. Schneider asserts that there three domains of combat: moral, cybernetic [mental], and physical. Domains can be affected by capabilities, to include EA. Combining these ideas, we arrive at a methodology for understanding how new electronic attack capabilities can be leveraged in Multi Domain Operations (see Figure 3). Taking the case studies into account, the task now is to consider how we may combine emerging EA systems with existing capabilities to create effects in the physical, cybernetic, and moral domains to support lethal, maneuver, and moral efforts.

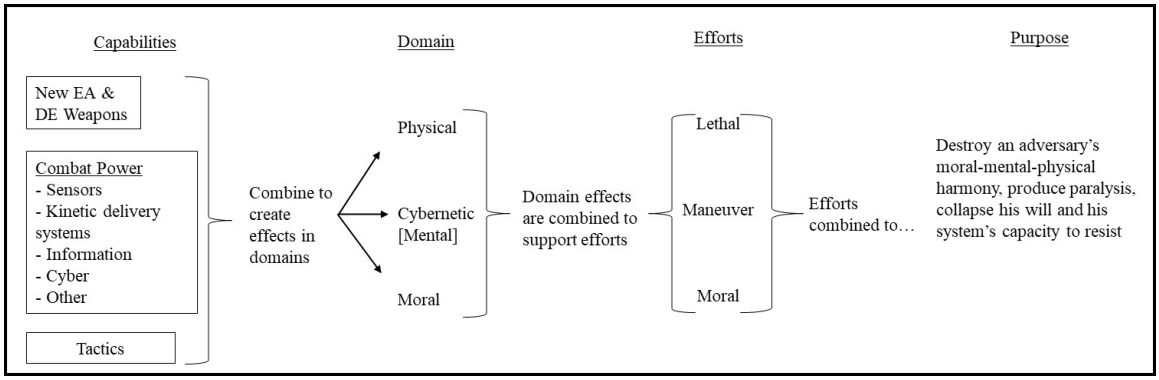

Figure 3. "Model for Applying Electronic Attack in Operations." Created by author.

Modern EA in the Physical Domain

The most significant change in the character of EW is the development of electronic weapons that can directly destroy enemy systems and platforms. HPM and HE laser systems have the capacity to destroy drones and aircraft. The Army's HE lasers are currently focused on air defense and counter-drone tasks, but it is only a matter time before those lasers are aimed at enemy platforms on the ground. The proliferation of active protection systems on combat vehicles, such as Israel's Trophy system, may require their suppression via jamming or DE

weapons before those platforms can be engaged with direct or indirect fire.[108] Equipping engineer units with a RADBO or similar HE laser system would allow them to rapidly reduce minefields, enabling faster ground maneuver during operations.

Drone swarm ES/EA jammers, operating in tandem with indirect or precision fire artillery, form a see-suppress-strike capability with the potential to operate far beyond the FLOT in support of reconnaissance and counter-reconnaissance missions. Aviation platforms armed with HE lasers would provide the Army with its longest-range direct fire weapon system, able to rise up for a line of sight shot miles from the target and then drop back to the ground. EMP artillery rounds would destroy the circuitry in active protection systems and counter-fire radars as part of conventional lethal strikes.

Army EA systems would also support other services in MDO in the physical domain. DE weapons have effects ceilings that could extend into space, allowing them to engage aircraft in support of the Air Force. Expendable drone jammers would activate enemy EA systems, revealing their location for Joint targeting. Special operations forces armed with small EMP devices could render shore-based radars and missile systems inoperable during littoral and maritime operations. Army HE lasers could potentially support the Space Force by targeting enemy satellites from the ground.

Modern EA in the Cybernetic Domain

While the US military has traditionally focused EA on the cybernetic domain, modern EA weapons offer land forces the potential to attack cybernetic decisive points along the length and breadth of the operational area. Swarming drones can extend the jamming range of Army divisions far beyond *AirLand Battle*'s 30km. ES systems could cue HE lasers to jam (or fry) antennas on command nodes. HPM and EMP munitions will render entire networks unusable,

[108] Vincent Delany, "On Killing Tanks," Modern War Institute, 23 Mar 2020, accessed 10 Dec 2020, https://mwi.usma.edu/on-killing-tanks/.

severely reducing a commander's ability to provide purpose and direction between distributed forces. Swarming EA drones and stationary decoys can simulate the electronic signatures of platforms and command nodes, deceiving the enemy and obfuscating his electronic surveillance efforts. The same capability could also flood the EMS with noise, hiding the employment or maneuver of key systems at critical times.

Drone jammers and HE lasers can suppress air defense systems in support of Air Force operations. EMP artillery is the perfect weapon for generating windows of maneuver in MDO, as it can neutralize non-emitting air defense radar without putting a manned airborne jammer at risk.[109] Ground jammers can break links between satellites and ground stations, freeing Space Force assets for other operations. EA systems can stimulate enemy networks or create openings that might facilitate cyber operations inside of the enemy network. The cumulative effects of EA against cybernetic decisive points will render an enemy unable to respond to accelerating lethal strikes or to counter penetrating maneuvers into vulnerable areas.

Modern EA in the Moral Domain

The Army can direct modern EA technology against an enemy's will at the tactical, operational, and strategic level. At the strategic level, EMP munitions could function as an effective deterrent against adversary action. EMPs launched from multiple vectors- air, space, sea, and land- provide escalation options short of nuclear exchange. At the operational level, a system that simulates cellular networks while jamming real ones, such as Russia's *Leer 3*, would help commanders manage the information environment more effectively. The employment of tactical EMPs against dispersed units, cut off electronically from their headquarters and adjacent formations, would generate fear and menace in less disciplined units. Laser-induced plasma effects could be employed during shaping operations, creating fear and anxiety as a prelude to

[109] Tim McGeehan, "Getting the Pulse of Multi-Domain Battle," Small Wars Journal, 15 Jul 2017, accessed 10 Dec 2020, https://smallwarsjournal.com/jrnl/art/getting-the-pulse-of-future-multi-domain-battle.

lethal kinetic strikes or a rapid penetrating maneuver.

As demonstrated by the Russians in Ukraine, manipulative electronic attack is a mechanism for exploiting intelligence gained during Joint cyber operations. Our cyber warriors must be integrated with EA and psychological operations to collect intelligence, craft a deception or message, and then project it wirelessly onto an adversary's network.

Recommendations

Researching and investing in new electronic weapons is just the beginning. Integrating them into a coherent warfighting system that engages in the EMS during all phases of MDO is just as important. We must rewrite our electronic warfare doctrine, organize these new capabilities into effective forces, and develop leaders to think and fight in the EMS.

Doctrine

The Army must consider how its EA systems may be combined with other forms of combat power to create effects in the physical, cybernetic, and moral domains. Our doctrine defines electronic attack as a form of fires, but it is a capability in and of itself. It functions within a broader multi-domain warfighting system to achieve operational and tactical objectives. Depending upon the desired effect, EA could be a supporting or a supported arm of the future combined arms fight. Mobile EA systems, such as drone jammers, will facilitate deception, enabling units to maneuver across the future battlefield. Air Force jammers could blind enemy radars to allow HE laser attack aviation to destroy critical targets. Class nine replacement batteries for EA systems may be set as a higher priority for distribution than class five ammunition in certain operations. Our doctrine must reflect how existing and emerging EA systems, independently or integrated with other forms of combat power, can destroy, deceive, isolate, menace, and demoralize the enemy on the multi-domain battlefield.

To address EW in MDO, TRADOC published TP 525-8-6, *Cyberspace and Electronic*

Warfare Operations, 2025-2040 in 2018.[110] This pamphlet does a thorough job of describing evolving threats and vulnerabilities in the EMS, as well as emphasizing the importance of integrating cyber and EW effects into operations. However, it affirms the Army's trend of combining cyber and EW into a single network-focused capability. Current doctrine and proposed concepts focus EA on Schneider's cybernetic domain: an adversary's networks, communications, and perceptions. But the proliferation of modern platforms with vulnerable integrated circuits and critical internal networks, combined with the emergence of powerful energy weapons, allow EA to engage independently in the physical domain. These developments should reframe our understanding of operations in the EMS and subsequently, our doctrine. They should also cause the Army to reconsider the role of other branches in stewarding our electronic warfare capability.

A key takeaway from this study is that emerging electronic attack systems are multirole. For example, the effects achieved by DE weapons are determined by proximity and power, meaning the difference between a physical or cybernetic effect. Aligning EA weapons to tactical tasks would be an effective way to manage EA resources during planning. The range and cross-domain effects of DE weapons, combined with interservice targeting networks, suggest that Army DE weapons could be apportioned for direct support missions to other services too.

The reactive nature of jamming and DE engagements between ground forces will severely limit the ability of higher headquarters to control the EMS. These battle drills will occur in the close fight, in close coordination between tactical EA and traditional maneuver units. While doctrine should still provide a procedural framework for spectrum management, it must also balance the increased risk of EM fratricide with the rapid pace of tactical electronic engagements.

The range of HE laser weapons could conceivably be limited only by the curvature of the Earth- an obstacle that an HE helicopter could overcome by increasing its altitude. This

[110] US Department of the Army, TRADOC Pamphlet 525-8-6, *Cyberspace and Electronic Warfare Operations, 2025-2040* (Washington, DC: Government Publishing Office, 2018).

development would render the designation of deep/close areas based upon weapon ranges less relevant than a deep/close designation based upon effects, time, and responsibilities. For example, a corps could task a subordinate division's EA assets to support Joint targeting in the corps deep area in one phase, with corps EA assets in general support to destroy enemy C2 in the division's deep area in the next phase. With the ability to engage deep targets with direct fire, *FMs 3-0* and *3-09* need to consider the role of division and below direct fire HE lasers in targeting operations. Maneuver units assigned or supported with high energy weapons must likewise be prepared to facilitate deep targeting and cross-domain fires.

Army Techniques Publications (ATPs) for tactical units should address how EA systems can support maneuver. Infantry, Stryker, and combined arms ATPs should include guidance for employing EA during all forms of the offense and defense, and cavalry ATPs must address how to incorporate ES and EA into all forms of reconnaissance and security. Air defense, mobility, counter-mobility, and Joint fires manuals must all be updated to reflect how DE can complement or replace existing tools in their respective functions.

Organization

The Army is on its way to developing viable MDO formations with its experimental Multidomain Task Force (MDTF). At the core of the MDTF is a battalion that prosecutes EA and cyber missions while fusing information and sensor data into targeting data for Joint fires.[111] This unit would possess the infrastructure and expertise to employ new EA capabilities, but the MDTF will likely be a theater asset. While some capabilities, such as EMP munitions with operational and strategic effects should be controlled by theater headquarters, other EA systems must reside in tactical organizations.

Tactical and theater air defense organizations need EA platforms to operate in tandem

[111] Kyle Borne, "Targeting in Multi-Domain Operations," *Military Review* (May-Jun 2019): 64-65, accessed 10 Dec 2020, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/.

with their radars and missile systems. It is possible that Stinger, Avenger, and Patriot missiles will be replaced by HPM and HE lasers entirely. It is also possible that air defense units will be required to serve in a counter-space role, defeating or jamming enemy satellites in addition to their protection function. Conflicts over training and manning as air defense transitions from missile operators to energy weapon operators could create friction between the Army's air defense and cyber branches.

ES/EA drones would function optimally with division or brigade reconnaissance squadrons, conducting recon, surveillance, jamming, and deception tasks in support of maneuver and targeting. HE laser countermine systems belong in maneuver enhancement brigades or brigade engineer battalions. Attack aviation armed with DE weapons would reside in aviation brigades, but likely also operate as part of a corps' long-range fires construct.

One advantage that the Russians and Chinese have over US expeditionary forces is established and hardened EW capability in friendly territory, postured to achieve immediate effects on US and NATO C4ISR.[112] To maintain an accurate electronic order of battle during competition and transition quickly to armed conflict, we must posture these new capabilities forward in theater-attached formations.

Leader Development and Education

During the years between the two World Wars, the French military rejected novel thinking about armored warfare, adopting a concept that proved inadequate against German operations in 1940. As the US Army reenters the arena of offensive EW, we must encourage subordinate leaders to think, create, and experiment with new applications of EA weapons across branches, warfighting functions, and echelons. Our leaders must start thinking about maneuver through the EMS now if we are to have the operational and tactical concepts necessary to win in the future.

[112] Clark, McNamara, and Walton, *Winning the Invisible War,* 28.

It is the author's experience from training and coaching at the National Training Center that leaders typically are not prepared to fight and survive in a contested EMS. Platoon and above certifications should simulate a contested EMS to meet requisite training outcomes. Company and above certifications should require the integration of EA enablers. Brigade, division, and corps warfighters should include cross-domain EA support to sister service operations. Regular integration of EA assets into company and battalion training will dispel the mystique surrounding Army EW assets and reinforce the lesson that the Army maneuvers through the EMS, as well as on land.

Entry-level professional military education should include blocks of instruction on the EMS and EW, US and adversary capabilities, and tactics and techniques to protect against EA. Career courses should reinforce these lessons and focus on the integration of EA weapons and capabilities within combined arms formations. Pairing education about the EMS with tactical decision games for junior leaders and staffs will reinforce classroom instruction.

Intermediate Level Education courses should educate staff leaders on division and corps roles and responsibilities in the EMS fight. Leaders need to understand how to use deceptive and offensive EA to shape the battlefield and manage the tempo of the fight. Attacking in the EMS must be done in consideration of phasing, transitions, and objectives, particularly when those effects intersect with information, psychological, and cyber operations. Crucially, leaders at this level must understand how the Army's new EA platforms and formations can be combined with Joint systems to generate greater capabilities.

To apply these lessons, we must develop realistic live, virtual, and constructive (LVC) training environments that replicate the effects of new capabilities in a contested EMS. Replicating the effects of new EA weapons will require a robust training paradigm for certifying exercises. Soldiers and leaders must acclimate to the novelty of invisible attacks, recognize the dangers of radiation from lasers and HPMs, understand the risks of using energy weapons while under electronic observation, and identify opportunities for deception and camouflage using EA

platforms.

Finally, leaders in every service and at all levels must be taught that our military maneuvers within the electronic and information domains, and we must attack and defend in the EMS to achieve victory on the modern battlefield. The Army must be cognizant of its previous EW atrophy as we move forward with the integration of EW into the cyber branch. We risk losing a conflict characterized by weapons that destroy networks if EW's current stewards are fixated on defending and fighting inside networks. Each branch should steward its own applications of EA and train its members to fight and lead in a contested EMS.

Conclusion

As the Joint Force transitions to All-Domain Operations (ADO), the Army must determine how it will use energy weapons to maneuver, survive, and support sister services. *AirLand Battle* and Russia's EMS tactics in the Donbass demonstrate an evolution in EA capabilities that should inform how we employ EW in MDO. New capabilities will allow the Army to apply electronic effects across multiple warfighting functions, along the breadth and depth of the battlefield. We must now equip, train, and lead in the EMS in earnest.

Further research should consider the implications of swarmed, autonomous EW technology in multidomain maneuver. The potential for long range EA systems, networked with machine learning or artificial intelligence, to dominate the EMS will require a multiservice approach for development and integration. Another study should examine the role and responsibilities of the services and branches in stewarding emerging EA capabilities. For instance, EMP weapons fit neatly into the "EA as a form of fires" category, but HE lasers would replace or complement direct fire munitions on mobile platforms. Maneuver, fires, and protection will all require close integration of EA capabilities, and their respective branches must be invested in EA development.

It is important to note that the United States is not the only nation weaponizing emerging

energy principles. Reports indicate that Russia is developing HPM and HE laser weapons to counter aerial threats.[113] Credible intelligence indicates that China possesses EMP weapons, and that its military recognizes their threat to US military platforms and civil infrastructure.[114] We should continue hardening existing systems against electronic attack, but not at the expense of fielding new offensive energy weapons. Our adversaries also rely upon the EMS.

The United States, China, and Russia all recognize that the combatant who dominates the EMS will prevail in modern state conflict. New technologies permit the US Army to inflict physical, cybernetic, and moral effects across all service domains. We must invest in the technology, doctrine, organization, and education of our leaders if we are to translate these breakthroughs into victory on the multidomain battlefield.

[113] Kjellen, *Russian Electronic Warfare,* 77.

[114] Peter Vincent Pry, *The People's Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack* (Washington, DC: EMP Task Force on National and Homeland Security, 2020), 4-5, accessed 4 Nov 2020, https://apps.dtic.mil/sti/ pdfs/AD1102202.pdf.

Bibliography

Ackerman, Spencer. "I Got Blasted by the Pentagon's Pain Ray—Twice." *Wired*. 12 Mar 2012. Accessed 4 Nov 2020. https://www.wired.com/2012/03/pain-ray-shot/.

Arcangelis, Mario de. *Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon* Conflicts. Dorset, United Kingdom: Blandford Press, 1985.

Atherton, Kelsey D. "Making Sense of CHAMP, the Silver Bullet Miracle Missile That Isn't." C4ISRNET. 13 Dec 2017. Accessed 6 Nov 2020. https://www.c4isrnet.com/ electronic-warfare/2017/12/13/making-sense-of-champ-the-silver-bullet-miracle-missile-that-isnt

Baker, Daniel. "Deep Attack: A Military Intelligence Task Force in Desert Storm." *Military Intelligence* 17, no. 4 (Oct-Dec 1991): 39-42. Accessed 14 Sep 2020. https://www.ikn.army.mil/apps/MIPBW/MIPB_Issues/MIPB%20Oct%201991.pdf#view=fit.

Bartles, Charles. "Role of Radio-Technical Troops in the Russian Armed Forces." *OE Watch* 06, no. 3 (March 2016): 50-52. Accessed 17 Sep 2020. https://community.apan.org/wg/tradoc-g2/fmso/m/oe-watch-past-issues/195441.

_____. "Recommendations for Intelligence Staffs Concerning Russian New Generation Warfare." *Military Intelligence Professional Bulletin* 43, no. 4 (Oct-Dec 2017): 10-17. Accessed 17 Sep 2020. https://www.ikn.army.mil/apps/MIPBW/MIPB_Issues/ MIPBOct_Dec17finalIKN.pdf#view=fit

Borne, Kyle D. "Targeting in Multi-Domain Operations." *Military Review* (May-Jun 2019): 61-67. Accessed 10 Dec 2020. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/.

Boyd, John R. *A Discourse on Winning and Losing*. Edited and Compiled by Grant T. Hammond. Maxwell Air Force Base, AL: Air University Press, 2018.

Clark, Bryan, Whitney Morgan McNamara and Timothy A. Walton. *Winning the Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum*. Washington, DC: Center for Strategic and Budgetary Assessments, 2019. Accessed 30 Aug 2020. https://csbaonline.org/research/ publications /winning-the-invisible-war-gaining-an-enduring-us-advantage-in-the-electromagnetic-spectrum.

Crane, Keith, Olga Oliker, and Brian Nichiporuk. *Trends in Russia's Armed Forces: An Overview of Budgets and Capabilities*. Santa Monica, California: RAND Corporation, 2019. Accessed 30 Aug 2020. https://www.rand.org/pubs/research_reports/RR2573.html.

Delany, Vincent. "On Killing Tanks." Modern War Institute. 23 Mar 2020. Accessed 10 Dec 2020. https://mwi.usma.edu/on-killing-tanks/.

Giles, Keir. "Handbook of Russian Information Warfare." Fellowship Monograph, Research Division, NATO Defense College, Rome, Italy, 2016.

George, Jonathan. "Marine Corps Electronic Warfare: We'll Figure it Out." *Marine Corps*

Gazette 102, no. 10 (October 2018): 14-18. Accessed 14 Sep 2020. https://mca-marines.org/wp-content/uploads/2018/12/MCG-October-2018-sm_0.pdf.

Keller, Jared. "The Army is Tripling the Power of One of its Vehicle-mounted Laser Systems." Task & Purpose. 8 May 2020. Accessed 4 Nov 2020. https://taskandpurpose.com/news/army-laser-weapon-power.

Keller, John. "Army Asks SRC to Build and Deploy Counter-Drone System to Protect Expeditionary Forces from Enemy UAVs." Military & Aerospace Electronics. 17 Jul 2020. Accessed 9 Oct 2020. https://www.militaryaerospace.com/unmanned/article/14180310/counterdrone-expeditionary-intelligence-gathering.

Kelly, Patrick, III. "The Electronic Pivot of Maneuver: The Military Intelligence Battalion (Combat Electronic Warfare Intelligence)." Masters Monograph, School of Advanced Military Studies, US Army Command and General Staff College, Ft. Leavenworth, KS, 1993.

King, Kenneth T. "Electronic Warfare and Organizational Encopresis: The Neglect of the US Army and Its Intelligence Branch to Advocate for Warfighting Capabilities in the Electromagnetic Spectrum." Masters Monograph, School of Advanced Military Studies, US Army Command and General Staff College, Ft. Leavenworth, KS, 2019.

Kjellan, Jonas. *Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces*. Stockholm, Sweden: Swedish Defence Research Agency (FOI). Accessed 16 Sep 2020. https://www.foi.se/en/foi/reports.html

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Jenny Oberholtzer, Andrew Radin, and Olesya Tkacheva. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Santa Monica, California: RAND Corporation, 2017. Accessed 10 Sep 2020. https://www.rand.org/pubs/research_reports/RR1498.html.

Lapaiev, Yuri. "Russian Electronic Warfare in Donbas: Training or Preparation for a Wider Attack?" *Eurasia Daily Monitor* 17, no. 34 (March 2020). Accessed 16 Sep 2020. https://jamestown.org/program/russian-electronic-warfare-in-donbas-training-or-preparation-for-a-wider-attack/.

Lawrence, D.B. "Soviet Radioelectronic Combat." *Air Force Magazine* 65, no. 3 (March 1982). Accessed 16 Sep 2020. https://www.airforcemag.com/article/0382radioelectronic/.

Loukianova, Anya. "Moscow's Emerging Electronic Warfare Capabilities: A Dangerous Jammer on U.S./NATO-Russian Relations?" Unpublished policy memo, Georgia Tech Program on Strategic Stability Evaluation, 2016. Accessed 17 Sep 2020. https://posse.gatech.edu/sites/default/files/pubfiles/Loukianova-Posse_Russian%20EW_final.pdf.

Maini, Anil K. *Handbook of Defence Electronic and Optronics: Fundamentals, Technologies, and Systems*. Hoboken, New Jersey: John Wiley & Sons, 2018.

McDermott, Roger N. *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*. Tallinn, Estonia: International Centre for Defence and Security, 2017. Accessed 30 Aug 2020. https://icds.ee/wpcontent/uploads/2018/ICDS_Report_Russias_Electronic_Warfare_to_2025.pdf.

McGeehan, Tim. “Getting the Pulse of Multi-Domain Battle.” Small Wars Journal. 15 Jul 2017. Accessed 10 Dec 2020. https://smallwarsjournal.com/jrnl/art/getting-the-pulse-of-future-multi-domain-battle.

Mehta, Aaron. “Air Force awards laser-armed RADBO contract to Parsons.” C4ISRNET. 25 Sep 2020. Accessed 4 Nov 2020. https://www.c4isrnet.com/industry/2020/09/25/air-force-awards-laser-armed-radbo-contract-to-parsons/.

Mizokami, Kyle. “The Navy Just Tested Its Most Powerful Laser Yet.” *Popular Mechanics*. 27 May 2020. Accessed 9 Oct 2020. https://www.popularmechanics.com/military/navy-ships/a32676643/navy-laser-weapon-system-demonstrator-test/.

Obering, Henry, III. “Directed Energy Weapons Are Real…And Disruptive.” *Prism* 8, no. 3 (October 2019): 38-46. Accessed 30 Aug 2020. https://ndupress.ndu.edu/Journals/PRISM/PRISM-8-3/.

Pomerleau, Mark. “Here’s How the Army is Grooming an Elite Cadre of (electronic) Cyber Soldiers.” Fifth Domain. 13 Sep 2018. Accessed 16 Sep 2020. https://www.fifthdomain.com/dod/army/2018/09/13/heres-how-the-army-is-grooming-and-elite-cadre-of-electronic-cyber-soldiers/.

Price, Alfred. *War in the Fourth Dimension: US Electronic Warfare from the Vietnam War to the Present*. London: Greenhill Books, 2001.

Pry, Peter V. *The People’s Republic of China Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack.* Washington, DC: EMP Task Force on National and Homeland Security, 2020. Accessed 4 Nov 2020. https://apps.dtic.mil/sti/pdfs/AD1102202.pdf

Rogoway, Tyler. “SPEAR Mini-Cruise Missile Getting An Electronic Warfare Variant To Swarm With Is A Huge Deal.” The Drive. 12 Sep 2019. Accessed 17 Sep 2020. https://www.thedrive.com/the-war-zone/29789/spear-mini-cruise-missile-getting-an-electronic-warfare-variant-to-swarm-with-is-a-huge-deal.

Romjue, John L. *From Active Defense to AirLand Battle: The Development of Army Doctrine 1973-1982*. Fort Monroe, VA: US Army Training and Doctrine Command, 1984.

_____. *A History of Army 86: Volume 1*. Fort Monroe, VA: US Army Training and Doctrine Command, 1983.

Schneider, James J. *Theoretical Paper No. 3: The Theory of Operational Art*. Fort Leavenworth, KS: US Army Command and General Staff College, 1988.

Smith, Patrick. *Russian Electronic Warfare: A Growing Threat to U.S. Battlefield Supremacy*. Washington, DC: American Security Project, 2020. Accessed 30 Aug 2020. https://www.americansecurityproject. org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf.

South, Todd. “Pentagon Scientists Are Making Talking Plasma Laser Balls for Use as Non-lethal Weapons.” *Military Times*. 19 Jul 2019. Accessed 4 Nov 2020. https://www.militarytimes.com /news/your-military/2019/07/19/pentagon-scientists-are-

making-talking-plasma-laser-balls-for-use-as-non-lethal-weapons/.

Trevithick, Joseph. “Air Force Set to Deploy Its Counter-Drone “Phaser” Microwave Weapon Overseas.” The Drive. 24 Sep 2019. Accessed 5 Nov 2020. https://www.thedrive.com/the-war-zone/29992/air-force-set-to-field-test-its-counter-drone-phaser-microwave-weapon-overseas-in-2020.

_____. “The Army Has Unveiled its Plan for Swarms of Electronic Warfare-Enabled Air-Launched Drones.” The Drive. 16 Aug 2020. Accessed 17 Sep 2020. https://www.thedrive.com/the-war-zone/35726/the-army-has-unveiled-its-plan-for-swarms-of-electronic-warfare-enabled-air-launched-drones.

_____. “Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio "Virus".” The Drive. 30 Oct 2019. Accessed 17 Sep 2020. https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus.

US Department of the Air Force. Air Force Annex 3-51, *Electromagnetic Warfare and Electromagnetic Spectrum Operations*. Washington, DC: Government Publishing Office, 2019.

US Department of the Army, 24th Mechanized Infantry Division Combat Team. *Operation Desert Storm, OPLAN 91-3.* Washington, DC: Government Printing Office, 1992.

US Department of the Army, Asymmetric Warfare Group. *Russian New Generation Warfare Handbook*. Washington, DC: Government Publishing Office, 2016.

US Department of the Army. Army Field Manual 3-09, *Field Artillery Operations and Fire Support.* Washington, DC: Government Publishing Office, 2014.

_____. Army Field Manual 3-12, *Cyberspace and Electronic Warfare Operations*. Washington, DC: Government Publishing Office, 2017.

_____. Army Field Manual 3-36, *Electronic Warfare in Operations*. Washington, DC: Government Printing Office, 2009.

_____. Army Field Manual 34-1, *Intelligence and Electronic Warfare Operations.* Washington, DC: Government Printing Office, 1987.

_____. Army Field Manual 100-5, *Operations.* Washington, DC: Government Printing Office, 1986.

_____. Army Field Manual 101-10-1, *Staff Officers’ Field Manual Organizational, Technical, and Logistical Data (Volume 1)*. Washington, DC: Government Printing Office, 1987.

———. Army Techniques Publication 3-12.3, *Electronic Warfare Techniques.* Washington, DC: Government Publishing Office, 2019.

_____. Army Techniques Publication 3-09.32, *Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower (JFIRE)*. Washington, DC: Government Publishing Office, 2019.

———. Training and Doctrine Command Pamphlet 525-3-1, *The U.S. Army in Multi-Domain Operations 2028.* Washington, DC: Government Publishing Office, 2018.

_____. Training and Doctrine Command Pamphlet 525-5, *The AirLand Battle and Corps 86*. Washington, DC: Government Printing Office, 1981.

_____. Training and Doctrine Command Pamphlet 525-8-6, *Cyberspace and Electronic Warfare Operations, 2025-2040.* Washington, DC: Government Publishing Office, 2018.

US Department of the Army, Combined Arms Combat Developments Activity. Memorandum describing the operational concept for heavy division operations on the 1986 battlefield. 8 Jul 1980. CACDA Files. Combined Arms Research Library, Fort Leavenworth, KS.

US Department of Defense. Joint Staff. Joint Publication 3-12, *Cyberspace Operations.* Washington, DC: Government Publishing Office, 2018.

_____. Joint Publication 3-13.1, *Electronic Warfare.* Washington, DC: Government Printing Office, 2012.

_____. Joint Publication 3-09, *Joint Fire Support*. Washington, DC: Government Publishing Office, 2019.

US Department of Defense. Office of the Under Secretary of Defense for Acquisition & Sustainment. DoD 2017.1 Small Business Innovation Research (SBIR) Solicitation. 30 Nov 2016. Accessed 16 Sep 2020. https://www.sbir.gov/node/1206543.

US Department of the Navy. Naval Doctrine Publication 1, *Naval Warfare*. Washington, DC: Government Publishing Office, 2020.

US Department of the Navy, United States Marine Corps. Marine Corps Reference Publication 3-32D.1, *Electronic Warfare*. Washington, DC: Government Publishing Office, 2018.

US Department of the Space Force. Space Capstone Publication, *Spacepower: Doctrine for Space Forces*. Washington, DC: Government Publishing Office, 2020.

US Library of Congress. Congressional Research Service. *Ground Electronic Warfare: Background and Issues for Congress*, by John R. Hoehn. R45919. 2019. Accessed 30 Aug 2020. https://fas.org/sgp/crs/weapons/R45919.pdf.

Walling, Eileen M. *High Power Microwaves: Strategic and Operational Implications for Warfare*. Maxwell Air Force Base, AL: Center for Strategy and Technology, Air War College, 2000. Accessed 15 Sep 2020. www.airuniversity.af.edu/Portals/10/CSAT/documents/OP/csat11.pdf

Work, Robert O., and Greg Grant. *Beating the Americans at their Own Game: An Offset Strategy with Chinese Characteristics*. Washington, DC: Center for New American Security, 2019. Accessed 30 Aug 2020. https://www.cnas.org/publications/reports/beating-the-americans-at-their-own-game.

Wiener, Norbert. *The Human Use of Human Beings: Cybernetics and Society*. Da Capo Series in

Science. 1954; repr., Boston: De Capo Series in Science, 1998.