Policy Options for Electromagnetic Spectrum Management in Support of Multi-Domain Operations

A Monograph

by

MAJ Nathaniel R. Welsh
US Army

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

2020

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
21-05-2020	Master's Thesis	JUN 2019 - MAY 2020

4. TITLE AND SUBTITLE

Policy Options for Electromagnetic Spectrum Management in Support of Multi-Domain Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

MAJ Nathaniel R. Welsh

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 ORGANIZATION 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 Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The electromagnetic spectrum provides the US Army the capability to communicate across vast distances with voice, data, and video, navigate using global positioning system (GPS) satellites and gain intelligence of enemy activity, etc. The US Army's electromagnetic spectrum use continues to increase while electronic warfare capabilities to defend the electromagnetic spectrum decreased. The research question purposed is how does the US Army control a contested electromagnetic spectrum to enable operational maneuver? The initial hypothesis posits the US Army develops a policy for electronic warfare which seeks to control the entirety of the electromagnetic spectrum. The policy is comprised of both materiel and non-materiel capability-based approaches which are necessary to dominate the electromagnetic spectrum in future warfare.

15. SUBJECT TERMS

Electromagnetic Spectrum (EMS), Electronic Warfare (EW), Multi-Domain Operations (MDO)

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			MAJ Nathaniel R. Welsh
(U)	(U)	(U)	(U)		19b. TELEPHONE NUMBER *(Include area code)*

Monograph Approval Page

Name of Candidate: MAJ Nathaniel R. Welsh

Monograph Title: Policy Options for Electromagnetic Spectrum Management in Support of Multi-Domain Operations

Approved by:

_____, Monograph Director
Adam B. Lowther, PhD

_____, Seminar Leader
David A. Meyer, COL

_____, Director, School of Advanced Military Studies
Brian A. Payne, COL

Accepted this 21st day of May 2020 by:

_____, Acting Director, Graduate Degree Programs
Prisco R. Hernandez, PhD

Abstract

Policy Options for Electromagnetic Spectrum Management in Support of Multi-Domain Operations, by MAJ Nathaniel R. Welsh, 34 pages.

The electromagnetic spectrum provides the US Army the capability to communicate across vast distances with voice, data, and video, navigate using global positioning system (GPS) satellites and gain intelligence of enemy activity, etc. The US Army's electromagnetic spectrum use continues to increase while electronic warfare capabilities to defend the electromagnetic spectrum decreased. The research question purposed is how does the US Army control a contested electromagnetic spectrum to enable operational maneuver? The initial hypothesis posits the US Army develops a policy for electronic warfare which seeks to control the entirety of the electromagnetic spectrum. The policy is comprised of both materiel and non-materiel capability-based approaches which are necessary to dominate the electromagnetic spectrum in future warfare.

Contents

Acknowledgements

Foremost, to Brenna and our boys Nate Jr. and Liam for their continued love and support throughout the many hours invested completing this endeavor.

Abbreviations

AM	Amplitude Modulation
EA	Electronic Attack
ELF	Extremely Low Frequency
EP	Electronic Protection
EMS	Electromagnetic Spectrum
EW	Electronic Warfare
EWS	Electronic Warfare Support
EHF	Extremely High Frequency
FM	Field Manual
FM	Frequency Modulation
GHz	Giga Hertz
GPS	Global Positioning System
HF	High Frequency
Hz	Hertz
INEW	Integrated Network Electronic Warfare
JP	Joint Publication
kHz	Kilo Hertz
LF	Low Frequency
Mbps	Megabits per second
MF	Medium Frequency
MHz	Mega Hertz
REC	Radio Electronic Combat
RCIED	Radio Controlled Improvised Explosive Device
SCADA	Supervisory Control and Data Acquisition
SDR	Software Defined Radio

SDS	Spectrum Dependent Systems
SHF	Super High Frequency
TP	TRADOC Publication
UFH	Ultra High Frequency
VLF	Very Low Frequency

Figures

Introduction

> Electronic warfare is intended to shut the ear, stop the voice, close the eyes and freeze the nervous system. Deaf, dumb, and paralyzed soldiers do not live long in battle.
>
> — Niel Munro, *The Quick and the Dead*

My initial interest in electronic warfare began as a young officer during a deployment to Afghanistan in 2013. It was there that I became familiar with numerous in-theatre electronic warfare systems specifically designed to counter radio-controlled improvised explosive devices (RCIED) and enemy radio communications. While these systems were adequate and operated as designed, their use frequently degraded radio communications making command and control of dismounted and mounted operations challenging from a command and control, fires, and intelligence perspective. The challenge to devise ways to manage the symbiotic relationship between protecting the force with electronic warfare systems while simultaneously fighting the enemy is a challenge without a simple solution. It is fair to say; initially, I had a myopic view of electronic warfare as it affected our limited area of operations. It was only after my assignment to the Army's Asymmetric Warfare Group (AWG) as a senior Captain, my aperture expanded to gain a holistic awareness of how vital control of the electromagnetic spectrum is to the Army.

The purpose of this monograph is to inform and educate fellow military professionals about the electromagnetic spectrum, which represents a vital component of multi-domain operations (MDO). Given electronic warfare is not a new concept, this work is proactively forward-leaning to highlight the increasingly complex competition between the civilian sector, the military, and the adversary. This work is not an attempt to delve into the specific tools or methods of electronic warfare but focuses on the deconfliction to minimize electromagnetic interference, which enables communication via electronic warfare.

The research question to support this endeavor is how does the Army control a contested electromagnetic spectrum to enable operational maneuver? The initial hypothesis associated with

the research question centered posits that the Army develops a policy for electronic warfare which seeks to control the entirety of the electromagnetic spectrum.

Background

Electronic warfare (EW) represents an under-appreciated and often misunderstood capability within the Army. At the height of the Cold War, the Army maintained robust ground-based electronic warfare capabilities as required to execute Air Land Battle. The 1991 Gulf War represented the apex of electronic warfare and the point of departure for understanding the role electronic warfare plays in future conflict. The Gulf War represents the apex because prior to Desert Storm, Russia was the primary threat and pacing nation for US capability development. During the Gulf War, the advent of the Global Positioning System (GPS) and precision-guided munitions represented only seven percent of all weapons employed by the United States but destroyed eighty percent of important targets.[1] During the 1991 Gulf War, the US military employed aerial and ground-based digital networks linked to precision-guided munitions, which increased lethality and decreased collateral damage. Since the 1991 Gulf War, adversaries in Afghanistan and Iraq were unable to challenge US superiority in the electromagnetic spectrum and as a result the United States divested EW systems and capabilities to fund emerging requirements.

During the same period, Russia and China invested heavily in modernizing electronic warfare capabilities to disrupt or disintegrate American command and control capabilities. The Russians adopted radio-electronic combat (REC) to destroy "thirty percent by jamming and thirty percent by destructive fires."[2] The Chinese developed integrated network electronic warfare (INEW), which is described as each side seeking to immobilize the other's communications, data,

[1] Larry M. Wortzel, “The Chinese People’s Liberation Army and Information Warfare,” *Strategic Studies Institute* (2014): 13, accessed September 15, 2019, http://www.jstor.org/stable/resrep11757.

[2] Ibid., 13.

command, and sensor network.[3] Competing within traditional military roles of the EMS is but one fight within the electromagnetic spectrum. As the twenty-first century continues, it is likely that the most complicated fight resides within the broader civilian usage of the EMS.

The EMS supports critical civilian infrastructure. The increasing proliferation and use of cellular networks, global positioning system (GPS), and wireless technology represents a few essential examples of the civilian use of the EMS. GPS alone aids "vehicle navigation and supports critical infrastructure by synchronizing a wide range of computer-based systems including, law enforcement, emergency services, transportation, communications, electrical power grids, and financial transactions."[4] In a developed country, their failure, incapacitation, or destruction would arbitrarily have a debilitating impact on the economic security, societal stability, and physical security aspects of a nation.[5] Due to the effect on civilian critical infrastructure, military forces utilizing electronic warfare effects must understand the implications of the Laws of Armed Conflict in accordance with the principles of discrimination, lawfulness, necessity, humanity, and neutrality. Adversarial forces utilizing civilian technology for military purposes pose an asymmetric threat to the US military. Ultimately, the convergence of the traditional roles of civilian and military utilization of the EMS represents an evolution of the character of warfare in the twenty-first century.

Significance

In 2014, it took three minutes for the Russian Army to destroy two Ukrainian armored battalions, thus rendering the Ukrainian brigade ineffective. The Russians' utilized electronic warfare to direction find (DF) signals then utilized a civilian small-unmanned aircraft system (s-

[3] Ibid., 12.

[4] Tegg Westbrook, "The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare," *Journal of Strategic Security*, 12, No. 2, (2019): 1, accessed September 15, 2019, https://www.jstor.org/stable/10.2307/26696257.

[5] Gillian Pye and M.J. Warren, "An Emergent Security Risk: Critical Infrastructures and Information Warfare" *Journal of Information Warfare* 8, no. 3 (2009): 2, accessed September 20, 2019, https://www.jstor.org/stable/10.2308/26486764.

UAS) to observe the presence of a Ukrainian command post. Once observed, the Russians employed traditional electronic warfare systems to jam Ukrainian C2 frequencies reducing the Ukrainian ability to coordinate with adjacent units, fixing the Ukrainians in place. With the Ukrainian's fixed in place, the Russians employed an overwhelming lethal bombardment of rocket and cannon artillery to destroy the Ukrainian position.[6] The destruction of two Ukrainian armored battalions in three minutes provides insight into a worst-case scenario in which a combined arms approach is taken to employ electronic warfare and fires. In response, the Army is racing to close capability gaps with significant modernization and procurement of electronic warfare capabilities to prevent a similar catastrophe from happening to American soldiers.

As the Army learned during insurgencies in Iraq and Afghanistan, the EMS is no longer for either military or civilian purposes alone. The increased civilian use of the EMS poses an asymmetrical threat by providing high-tech and low-cost alternatives to conventional military capabilities. Remote-controlled improvised explosive devices (RC-IED) is only one example to illustrate the capability of asymmetric threats posed by civilian technology on military operations.

Successful control of the EMS denies an adversary's use of the EMS while preserving its availability for friendly use through the use of electronic warfare.[7] The policy recommendation for the Army comprises the full range of the EMS, both military and civilian, to enable operational maneuver.

Literature Review

> To achieve victory we must as far as possible make the enemy blind and deaf by sealing his eyes and ears, and drive his commanders to distraction by creating confusion in their minds.

---

[6] MG Patricia Frost, CPT Clifton McClung, LTC Christopher Walls, ed. LTC Daniel Huynh, "Tactical Considerations to Fight and Win in the Electromagnetic Spectrum," *The Cyber Defense Review* 3, no.1 (Spring 2018): 15, accessed September 21, 2019, https://www.jstor.org/stable/10.2307/26427371.

[7] B van Nierkerk and M. Maharaj, "The Future Roles of Electronic Warfare in the Information Warfare Spectrum," *Journal of Information Warfare* 8, no. 3 (2009): 2, accessed September 2, 2019, https://jstor.org/stable/10.2307/26486763.

— Mao Tse-Tung

Civilian Use of the EMS

The professional body of knowledge on electronic warfare illustrates the competition for control of the finite resource of the electromagnetic spectrum. The civilian sector, the military, and an adversary comprise the three primary groups competing for space within the electromagnetic spectrum. Particular emphasis is given to the civilian sector to emphasize the interconnectedness between the three groups to highlight the second and third-order effects of electronic warfare on the civilian population.

Gillian Pye and M.J. Warren focus on the civilian sector and critical civilian infrastructure and the vital role of global positioning system (GPS) and wireless technology fulfills in modern society. Critical infrastructure is defined as systems or capabilities which are indispensable to normal societal day-to-day living expectations and that their failure, incapacitation, or destruction would arbitrarily have a debilitating impact on the entire economic security, social stability, and physical security aspects of a nation.[8] The spectrum dependent systems (SDS) which tie these systems together is the GPS network and wireless technology.

Tegg Westbrook focuses on the GPS network writing that GPS is not only used to aid navigation in vehicles, it supports critical infrastructure by synchronizing a wide range of computer-based systems, including law enforcement, emergency services, transportation, communications, electrical power grids, and financial transactions, amongst many others.[9] The GPS is a satellite-based system that provides the position, navigation, and timing to a range of applications supporting the critical infrastructure of personal navigation in vehicles.

---

[8] Pye and Warren, "An Emergent Security Risk: Critical Infrastructures and Information Warfare," 2.

[9] Westbrook, "The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare," 1.

Marc J. O'Connor provides the final facet of the civilian use of the EMS focusing on wireless technology. The wireless technology is a primary means to connect communication devices to the internet. Technological developments in the final decade of the twentieth century provided access to the internet and then wireless technology (WiFi) on 802.1x frequency for data, streaming high-quality videos, and radio-controlled devices to name a few.[10] Where wireless technology provides ease of access and transmission of data, wireless transmitters are susceptible to direction finding and are easily interfered with via electronic warfare.

After developing an understanding of the civilian government's use of the EMS is it possible to explore the impact of interference on the critical infrastructure. Marc J. O'Connor emphasizes the critical infrastructure (SCADA, Air Traffic Control, Emergency Services) which all utilize wireless and GPS technology. Supervisory control and data acquisition (SCADA) systems monitor infrastructure parameters, such as temperature, flow rate and system alarms. A natural gas pipeline employs SCADA network to operate valves and monitor pipeline pressure. Air traffic control requires wireless communications between aircraft and controllers. Interruptions in communications can delay and degrade airport operations since they enter a "fail-safe" condition, suspending activity. Lastly, emergency services rely upon wireless communication in the form of a Land Mobile Radio (LMR) for tactical communications in order to coordinate services and inform emergency responders. This includes ground and air-based security forces, pre-hospital care, marine security, and fire department communication.[11]

Adversary Electronic Warfare

The Foreign Military Studies Office analysis on *The Russian Way of War* highlights the 2008 Russo-Georgia War as the stimulus and renewed focus in the development of advanced

[10] Marc J. O'Connor, "Electronic Warfare for the Fourth Generation Practitioner," *Small Wars Journal*: 6, accessed on November 29, 2019, https://smallwarsjournal.com/jrnl/art/electronic-warfare-fourth-generation-practitioner.

[11] O'Connor, "Electronic Warfare and the Fourth Generation Practitioner," 7.

electronic warfare equipment due to the loss of five aircraft in the first days of the conflict. In addition to advanced electronic warfare systems, the Russians also implemented organizational and personnel changes to optimize the technology. Most notably, the Russians had dedicated electronic warfare companies, battalions, and brigades. In contrast to the Army and Marine Corps who have relatively few electronic warfare systems, the Russians have an abundance of ground-based electronic warfare systems capable of operating at the tactical, operational, and strategic levels. Russian electronic warfare capabilities include wide-area cellular communications jamming, GPS location spoofing, reconnaissance, and communication satellite jamming, and disrupting early waring aircraft such as the E-3 Sentry (AWACS).[12]

In 2014, Russia demonstrated the post-2008 modernization effort in Ukraine which served as the basis for MG Frost's article in the *Cyber Defense Review* "Tactical Considerations to Fight and Win in the Electromagnetic Spectrum." The Russians' utilized electronic warfare to DF signals then utilized a civilian s-UAS to observe the presence of a Ukrainian command post. Once observed, the Russians employed traditional electronic warfare systems to jam Ukrainian C2 frequencies reducing the Ukrainian ability to coordinate with adjacent units, fixing the Ukrainians in place. With the Ukrainian's fixed in place, the Russians employed an overwhelming lethal bombardment of rocket and cannon artillery to destroy the Ukrainian position.[13]

Additionally, Westbrook highlights additional instances of multiple adversaries utilization of electronic warfare. In 2001, Iran spoofed and captured a US RQ-170 Sentinel Unmanned Aerial Vehicle (UAV) by redirecting it to land inside Iranian borders. North Korea targeted military and civilian air and naval traffic near the demilitarized zone with Russian-designed military jammers on more than one hundred occasions. This jamming reportedly

[12] Dr. Lester W. Grau and Charles K. Bartles, "The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces," *Foreign Military Studies Office,* (2016): 290, accessed November 10, 2017, https://community.apan.org/wg/tradoc-g2/fmso/p/fmso-bookshelf.

[13] Frost, McClung, and Walls, "Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum," 15.

affected over 1,000 civilian aircraft, hundreds of fishing vessels, cell phone services, and car navigation services. In September 2017, Norwegian airliners had to navigate with the help of radio signals due to the loss of GPS when the entered the East Finnmark airspace due to ongoing Russian military exercises.[14]

As the Army reliance on the electromagnetic spectrum increased to improve intelligence, precision fires, and command and control our adversaries developed technologies to degrade or deny those capabilities.

US Army Electronic Warfare

Beginning with the publication of the Department of Defense Electromagnetic spectrum Strategy in 2013, the electronic warfare across DoD is undergoing a renaissance and renewed focus in electronic warfare post operations in Iraq and Afghanistan. The demand for more and timely information at every echelon is driving an increase in DoD's need for spectrum. Increasingly lower echelons, including individual soldiers, require situational awareness information resulting in more spectrum-enabled network links. The growth in the complexity of modern military systems has similarly led to an increase in spectrum requirements.[15]

The Congressional Research Service in *Defense Primer: Electronic Warfare* published in 2019 lists the role of electronic warfare in military operations. In a contested environment, electronic warfare ensures the electromagnetic spectrum for radio frequencies to communicate with friendly forces, microwaves for tactical datalinks, radars, and satellite communications, infrared for intelligence and to enemy targeting, and lasers across the entire spectrum to communicate, transmit data, and potentially destroy a target. Specific to the Army are terrestrial electronic warfare sensors and jammers, which are limited by the amount of power available and

[14] Westbrook, "The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare," 7.

[15] Department of Defense, "Electromagnetic Spectrum Strategy 2013: A Call to Action," accessed on November 10, 2019, https://dodcio.defense.gov/Portals/0/Documents/Spectrum/ESS.pdf.

variance in terrain. Ground electronic warfare capabilities were traditionally used to intercept and to jam radios and artillery radars. More recent uses include jamming RCIEDs in Iraq and Afghanistan with mounted and dismounted systems.[16]

On December 6, 2018, when the Army published TRADOC Pamphlet 525-3-1 *The U.S. Army in Multi-Domain Operations 2028*, electronic warfare was thrust to the forefront with renewed purpose in preparing for near-peer combat operations. The first of four problems in the emerging operational environment that MDO seeks to address particular to electronic warfare was that "adversaries are contesting all domains, the electromagnetic spectrum (EMS), and the information environment and US dominance is not assured."[17] As a concept, "the central idea of MDO is the rapid and continuous integration of all domains of warfare to deter and prevail as we compete short of armed conflict. If deterrence fails, Army formations,[...], penetrate and dis-integrate enemy anti-access and area denial systems; exploit the resulting freedom of maneuver to defeat enemy systems, formations, and objectives and to achieve our own strategic objectives; and consolidate gains to force a return to competition on terms more favorable to the U.S., our allies and partners."[18] Convergence is a central tenant of MDO, defined as the rapid and continuous integration of capabilities in all domains, the EMS, and the information environment that optimizes effects to overmatch the enemy through cross-domain synergy and multiple forms of attack.[19] Lastly, cross-domain synergy “optimizes capabilities from across all domains, the EMS, and the information environment to achieve the maximum effect from the available resources.”[20]

---

[16] US Library of Congress, Congressional Research Service, *Defense Primer: Electronic Warfare*, by John R. Hoehn, IL11118 (September 18,2019), accessed November 10, 2019, https://fas.org/sgp/crs/natsec/IF11118.pdf.

[17] US Department of the Army, TRADOC Pamphlet (TP) 525-3-1, *The U.S. Army in Multi-Domain Operations 2028* (Washington, DC: Government Printing Office, 2018), vi.

[18] US Army, TP 525-3-1*,* iii.

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

[20] US Army, TP 525-3-1, 21.

The following year, the Army published the *2019 Army Modernization Strategy: Investing in the Future,* which lists six modernization priorities to conduct multi-domain operations by 2028. The fourth modernization effort is the modernization of the Army network technology to command and control forces distributed across vast, terrain, converge effects from multiple domains, and maintain a common situation understanding. Corresponding to the modernization efforts are the eight cross-functional teams plus two enabling areas in which one focuses on assured positioning, navigation, and timing (GPS).[21]

The Electromagnetic Spectrum

The modern world in the information age depends on the electromagnetic spectrum in common uses such as radio stations, television remotes, cellular phone text messages, television, microwave ovens, and medical x-rays. Electromagnetic radiation is depicted on the electromagnetic spectrum in accordance with their increasing wavelength from very long radio waves measured in meters on one end to microwaves, infrared light waves, visible light rays, ultra-violet rays, x-rays, and the very short gamma rays measured in nanometers on the opposite end of radio waves.

[21] US Department of the Army, "2019 Army Modernization Strategy: Investing in the Future," accessed on November 10, 2019, https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf.

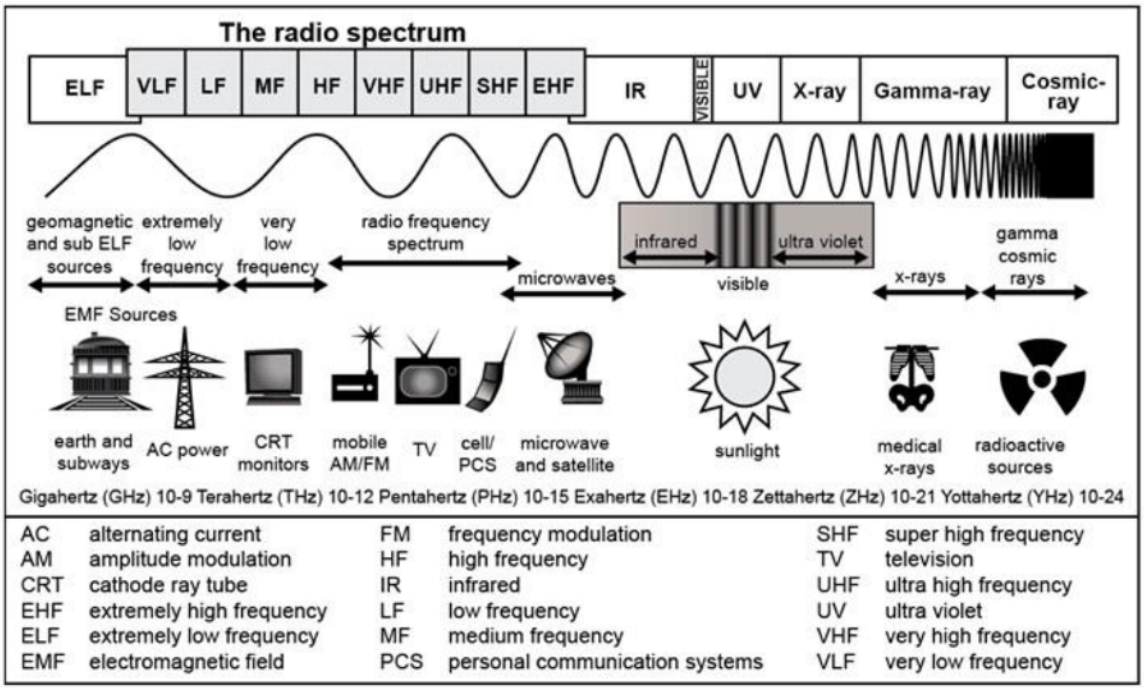

Figure 1. The Electromagnetic Spectrum, US Department of the Army, Field Manual (FM) 3-12, *Cyberspace and Electronic Warfare Operations Fundamentals* (Washington, DC: Government Printing Office, 2017), 1-12.

If electromagnetic energy is visualized as ocean waves, the length of an electromagnetic wave is the distance between one wave peak to the next peak, or from on wave trough to the next trough. The actual wavelength of electromagnetic waves varies from hundreds of kilometers one end of the electromagnetic spectrum to billionths of a single meter (nanometers) and even less on the other end. Most of the electromagnetic energy used by the military has wavelengths from a few tens of meters to a few thousandths of a meter.[22] The criteria for selection of a particular waveform depends primarily on the desired function of the signal and the environmental and atmospheric properties which the signal travels.

[22] Munro, *The Quick and the Dead*, 2.

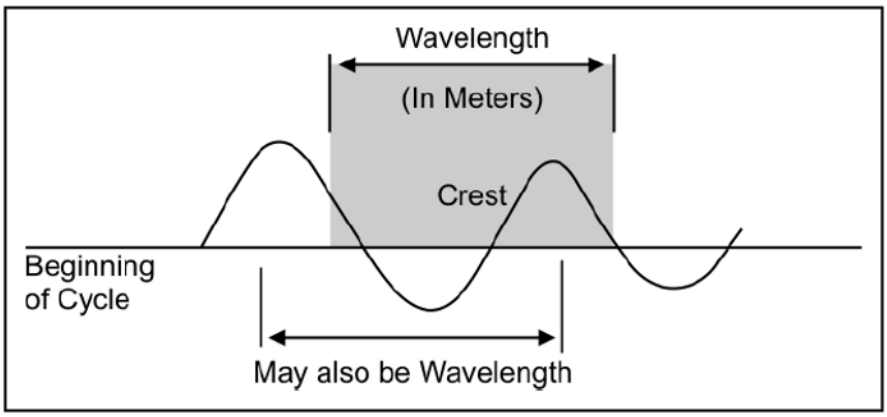

Figure 2. Wavelength, US Department of the Army, Army Techniques Publication (ATP) 6-02.53, *Techniques for Tactical Radio Operations* (Washington, DC: Government Printing Office, 2016), B-3.

How often complete waves pass a fixpoint in one second is the frequency. Because all electromagnetic energy travels at the speed of light, the shorter the wavelength, the more frequently waves pass a fixed point. In other words, the shorter the wavelength, the higher the frequency, and correspondingly, the longer the wavelength, the lower the frequency.[23] Hertz (Hz) measures frequency, in which one Hz equals one cycle per second.

Lastly, because the electromagnetic spectrum is a limited resource, electronic communication involves trade-offs between accuracy, transmission speed, and quality. Bandwidth is the space on the spectrum and is measured in Hertz (Hz), one Hz equals one cycle per second.[24]

Military Use of the Electromagnetic Spectrum

Within the larger electromagnetic spectrum, the Army capabilities reside within the federally controlled spectrum for intelligence, communication, positioning navigation and timing (PNT), sensing, and command and control (C2).[25] Broadly speaking there are three different ways to use the electromagnetic spectrum for war communications, surveillance, and weapons

[23] Munro, *The Quick and the Dead*, 3.

[24] Ibid., 62.

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

guidance.[26] It is important to first develop an understanding of the Army's use of the electromagnetic spectrum in order to identify the methods available with electronic warfare to protect its use while denying it to our adversaries.

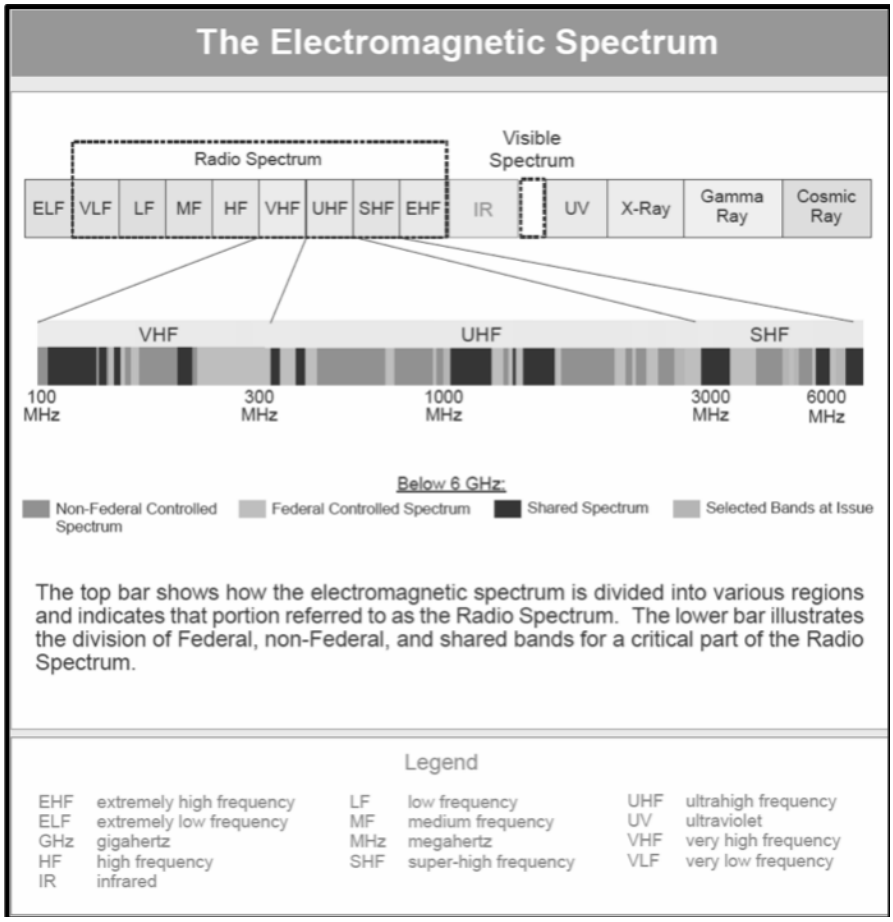

Figure 3. Radio Spectrum. US Department of Defense, Joint Staff, Joint Publication (JP) 3-13.1, Electronic Warfare (Washington, DC: Government Printing Office, 2012), 1-1.

For military purposes, one of the most important properties of any particular region or band is how well it travels through the atmosphere. For example, some radio waves travel around the world despite rain and wind, while infrared energy is absorbed before it can travel far.[27]

[26] Munro, *The Quick and the Dead*, 1.

[27] US Library of Congress, Congressional Research Service, *Defense Primer: Military Use of the Electromagnetic Spectrum*, by John R. Hoehn, IF11115 (May 24, 2019), accessed January 28, 2020, https://fas.org/sgp/crs/natsec/IF11155.pdf.

Within the radio spectrum, eight frequency bands provide varying capabilities, particular to military operations.

At the lower end of the radio frequency spectrum Extremely Low Frequency (ELF) 3-30 Hz, Very Low Frequency (VLF) 3-30 kHz, and Low Frequency (LF) 30-300 kHz low energy radio signals travel in long wavelengths. The antenna length, comparatively low-data transmission rates compared to very high frequency (VHF), make it an unsuitable band for tactical communications.[28]

Medium Frequency (MF) 30-3,000 kHz, combine short-range and relatively low bandwidth to render them of little military value for communications. Most often, commercial amplitude modulated (AM) radio stations comprise the medium frequency spectrum range.[29]

High Frequency (HF) 3-30 MHz, is widely used by the military for long-range radio transmissions because of its large bandwidth and high data rate. HF signals require only a few watts of transmitting energy to carry around the world. As an advantage, HF cheaply transmits signals from a small, low-power whip antenna to receivers all over the world. Conversely, HF is very vulnerable to disruptions in atmospheric conditions such as humidity and seasonal effects, to name a few. Secondly, given the easy which HF signals transmit allows for enemy eavesdropping and jamming, and possible wartime overcrowding of the band.[30]Prior to the development of satellite-based communications HF was the only method of long-range radio communication.[31]

Very High Frequency (VHF) 30-300 MHz has a range of 40-50 km and is achieved by a line of sight wave propagation with larger bandwidth, higher data rate, and more channels, and a smaller antenna than HF. VHF is ideally suited for the tactical line of sight communications that

---

[28] Munro, *The Quick and the Dead*, 63.

[29] Ibid., 65.

[30] Ibid., 66.

[31] Doug Richardson, *An Illustrated Guide to the Techniques and Equipment of Electronic Warfare* (New York, NY: Arco Publishing, 1985), 13.

link ground units. VHF signals degrade by intervening terrain and cannot transmit behind or through obstacles. As a result, troops with VHF systems are forced to maintain alternative communication links, including landline telephones or radio-relay transmitters, for use when VHF communication is blocked.[32]

Ultra-High Frequency (UHF) 300-3,000 MHz signals transmit up to a few tens of kilometers and share similar characteristics, advantages, and disadvantages of VHF with the added new capability of communications relay via satellite in space. UHF, unlike HF, is less prone to atmospheric conditions of the ever-changing ionosphere.[33]

Super High Frequency (SHF) 3-30 GHz signals often referred to as microwave transmission also travels by line of sight. The most critical added characteristic of these frequencies is their ability to be focused by a small dish antenna into a narrow beam with a divergence of only a few degrees. The main advantage of this narrow transmission path is the difficult for the enemy to intercept due to the narrow beam. Consequently, superhigh frequency signals can degrade after only several kilometers of passage through the air. With fog or rain, the problem rapidly becomes greater. High-power transmitters and sensitive receivers compensate for these losses, although at great expense.[34]

Extremely High Frequency (EHF) 30-100 GHz onboard the Advanced Extremely High Frequency Satellite (AEHF) is a strategic satellite-based capability operating at the highest end of the radio spectrum. The AEHFS provides global, survivable, secure, protected, and jam-resistant communications for top priority joint operations. AEHF represents the strategic communications backbone of the US military and while exceptionally vital is outside the tactical and operational scope.

---

[32] Munro, *The Quick and the Dead,* 66.

[33] Ibid., 65.

[34] Ibid., 67.

To conclude, electromagnetic radiation serves an important dual role in modern everyday life in the information age but also serves as a vital link to military operations specifically within the radio frequency bands in the electromagnetic spectrum. The electromagnetic spectrum is a finite resource with multiple competing interests between civilians (government, commercial, and private) and competing militaries. Both groups seek uninterrupted access, more data, and faster transmissions to gain a competitive advantage for business or military advantage over competitors.

Electronic Warfare

> Electronic warfare is military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy.
>
> — JP 3-13, *Electronic Warfare*

The Army employs advanced information and communications technology to integrate and synchronize intelligence, fires, protection, and command and control capabilities to decisively defeat or destroy adversaries. The effective integration and synchronization of these capabilities is the purpose of the Army's electronic warfare to deny the electromagnetic spectrum to the adversary while retaining its use to our own. Electronic warfare is the capability that represents a set of measures and actions for the detection and jamming of electronic systems for the control of forces and weapons, as well as for the electronic protection of one's electronic systems against technical reconnaissance, jamming, and interference. Electronic warfare comprises three distinct roles Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (EWS).

Electronic Attack (EA) involves the "use of electromagnetic energy or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability."[35]

Electronic Protection (EP) are "actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability."[36]

Electronic Warfare Support (EWS) are "actions taken by or under the direct control of an operational commander to search for, intercept, identify, and locate sources of intentional and unintended radiated electromagnetic energy."[37]

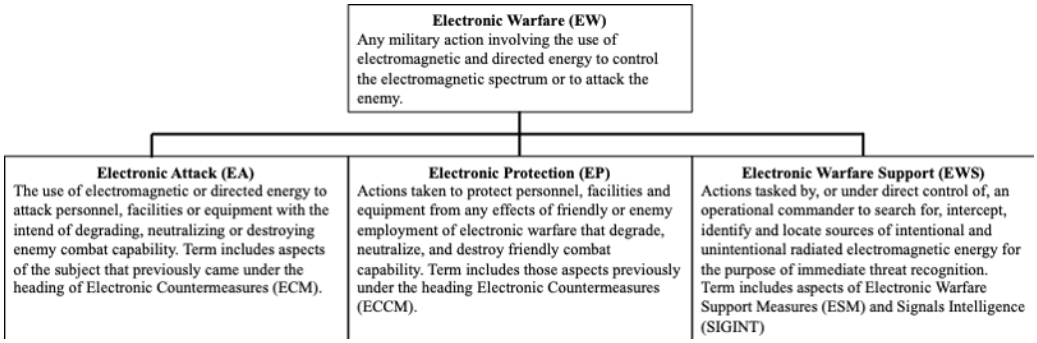

Figure 4. Electronic Warfare Hierarchy. Sergei A. Vakin, Lev N. Shustov, and Robert H. Dunwell, *Fundamentals of Electronic Warfare* (Boston, MA: Artech House, 2001), 2.

While Electronic Attack (EA) and Electronic Protection (EP) are no less critical, the Electronic Warfare Support (EWS) performs the vital role to sense, intercept, identify, and locate the sources of electromagnetic energy. To accomplish this task, the army uses an array of active and passive sensors.

Active sensors, radars, transmit, and receive electromagnetic energy and are the eyes and ears of the Army and are capable of detecting targets at hundreds of miles in range. The main disadvantage of active sensors is they are active sensors and so emits radio wave energy, much

[35] Sergei A. Vakin, Lev N. Shustov, and Robert H. Dunwell, *Fundamentals of Electronic Warfare* (Boston, MA: Artech House, 2001), 2.

[36] Ibid., 2.

[37] Ibid., 3.

like a searchlight emits visible light, which allows the enemy to locate the radar and counterattack.

Passive sensors are sensitive receivers and do not emit any energy. The main advantage of passive systems is they are difficult to detect, disrupt, or destroy. The disadvantage of passive sensors is they rely on the enemy stimulus to work. If the enemy minimizes their signals or even suppresses them entirely, the passive receiver does not detect a signal. However, given the proliferation of modern information technology in the form of radars and radios on the modern battlefield, adversaries are capable of minimizing their signature but less likely to suppress them entirely for a prolonged period.

Ultimately, Electronic Warfare Support (EWS) with active and passive sensors assist the commander in navigating the two critical dilemmas of dispersion and mass on the battlefield. Dispersion ensures survival from the adversary's advanced long-range weaponry. The only way to overcome the adversary is to combine forces and mass firepower at the critical time to win. While dispersion increase survivability in an electromagnetic degraded environment control of even well-organized forces degrades because the information is difficult to gather, orders are hard to communicate, and there is so little time to respond to fast, overwhelming and destructive fires.

Richard Kugler's Policy Options for Single Goals

> The greatest danger to technology intensive C3I networks is enemy electronic combat operations, which can destroy headquarters, jam communications, blind sensors, deceive intelligence analysts, slow decision-making and even cause a very swift collapse of the C3I networks, bought so expensively in peacetime.
>
> —Niel Munro, *The Quick and the Dead*

Step 1: Develop a Conceptual Framework

The conceptual framework utilized to follow Richard Kugler's policy options for single goals aligns with the framework of chapter one's literature review. The Army, the civilian sector and the adversary's use of the EMS comprise the three competing interests for bandwidth within

the EMS. Figure 5 from JP 3-13.1 represents the doctrinal foundation which highlight the interconnectedness of the electromagnetic spectrum and how both friendly and adversaries alike compete within the larger civilian sector.

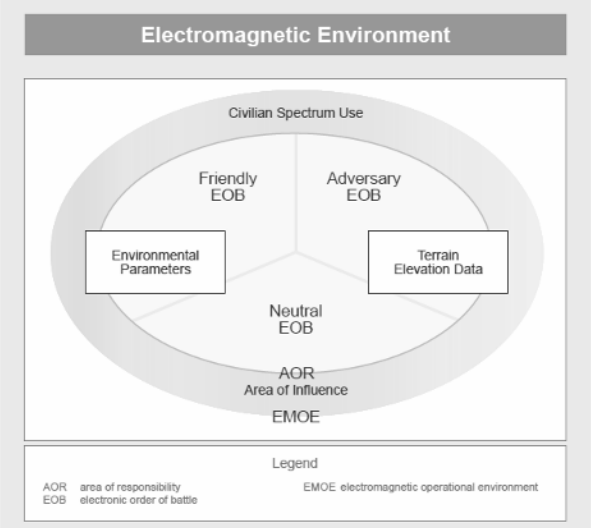

Figure 5. Conceptual Framework for the Electromagnetic Environment, US Department of Defense, Joint Staff, Joint Publication (JP) 3-13.1, *Electronic Warfare* (Washington, DC: Government Printing Office, 2012), 1-3.

Define the Problem

The nature of the problem derives from the imperative to synchronize the dispersion and mass of geographically separated units in time and space. Desynchronization of dispersion and mass and provides an adversary the opportunity to overwhelm and destroy in detail small isolated forces while avoiding the strength of the main force. In adherence to this imperative, the Army leverages information technology utilizing the EMS to send and receive real-time information to enable fires and maneuver. An adversary denying, degrading, or destroying the means to communicate through the use of electronic warfare desynchronizes the unit's ability to mass and disperse.

To contextualize the problem in a real-world scenario, picture a forward-positioned infantry unit in open terrain and outnumbered by enemy forces. Suddenly the infantry unit finds itself with no radio, sensors, electronics, or GPS. With communications jammed, disabled, and rendered useless, the infantry unit finds itself isolated and vulnerable to lethal air and ground

attacks. At this point, the infantry unit relies solely on organic weapon systems and is unable to request artillery support, aviation assets, or request reinforcement from an adjacent unit. While this may represent a worst-case scenario, it is not too far outside the realm of possibility given adversaries' current capabilities.

The origin of the problem began during the 1990 Gulf War and increased exponentially during each successive American conflict since. Operation Desert Storm first introduced network-enabled communication systems that transmitted and received vast amounts of battlefield information from maneuver units to operational headquarters in near real-time. Advanced communication systems fielded across units at echelon provided the Army an asymmetric advantage in terms of operational tempo and precision firepower to destroy adversaries quickly. Post-Gulf War the advent of the internet and wireless technology provided additional capabilities and means to further reduce the fog of war. As the Army's appetite for information increased exponentially the adversary in the 1990 Gulf War and later War on Terror had limited means to deny the Army's use of the EMS. As a result, the Army's electronic warfare capabilities in terms of technology and training atrophied while the Army's use increased exponentially turning a once asymmetric advantage into a potential vulnerability. Figure 6 below provides the actual spectrum use during the 1990 Gulf War and a projection of DoD Spectrum use for 2020.

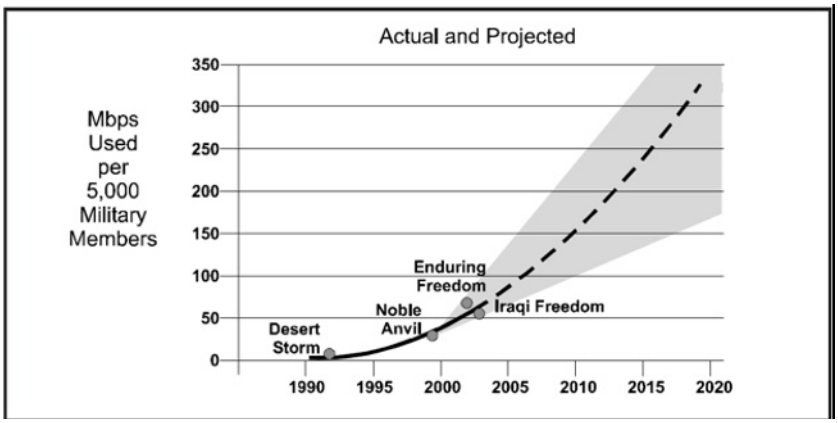

Figure 6. DoD Spectrum Requirements, US Department of Defense, “Electromagnetic Spectrum Strategy 2013: A Call to Action,” accessed December 26, 2019, https://dodcio.defense.gov/Portals/0/Documents/Spectrum/ESS.pdf.

Fast forward, to the present day in the United States, according to the Wireless Association, there were 198 million smartphones in the United States in 2016 and mobile traffic is expected to increase by 1,500% by 2020.[38] In a similar fashion, the Department of Defense continues to network large numbers of mobile devices and transmit vast amounts of data around the battlespace has created similar demands on spectrum access. Both 2G and 3G cellular phones operate at 850 MHz uplink and 1900 MHz downlink with an average transmission speed of 0-5 Mbps. 4G cell phones operate mainly at 1700 MHz uplink and 2100 MHz downlink with an average transmission speed of 5-12 Mbps.[39] The 4G waveform exists in a desirable section of the EMS with higher data rates but in the same frequency range as military radio frequencies. The EMS represents a shared commodity between the military and civilians each competing for greater access and share of the EMS for their respective purposes.

Figure 7 provided below is important because it provides the graphical depiction of the competition between the civilian sector and the military within the electromagnetic spectrum. Military systems are disadvantaged because military radios are constrained in capability due to the requirement to be portable (size and weight considerations), utilize omni-directional antennas, and be able to operate in austere areas without civilian communication infrastructure. To make more room within the EMS the military divides each frequency into quarters to deconflict radio traffic between echelons and increase the number of radios able to operate. The bottom line is a limit exists where the EMS physically cannot support that number of radios, regardless if the military is frequency hopping or not. The Army's research and development efforts are ongoing to create new waveforms and algorithms designed to operate within a contested EMS.

---

[38] US Defense Information System Agency (DISA), Strategic Planning Division, *Spectrum Strategic Planning Support*, accessed January 28, 2020, https://disa.mil/-/media/Files/DISA/Services/DSO/StrategicPlanningDivision.ashx?la=en&hash=49BB44D47115E5F147D926A347D131831AF06AEA.

[39] M.S. Marwick, "Analysis of Soldier Radio Waveform Performance in Operational Test," Institute for Defense Analyses (May 2015): 64, accessed on October 31, 2019, https://apps.dtic.mil/dtic/tr/fulltext/u2/1032264.pdf.

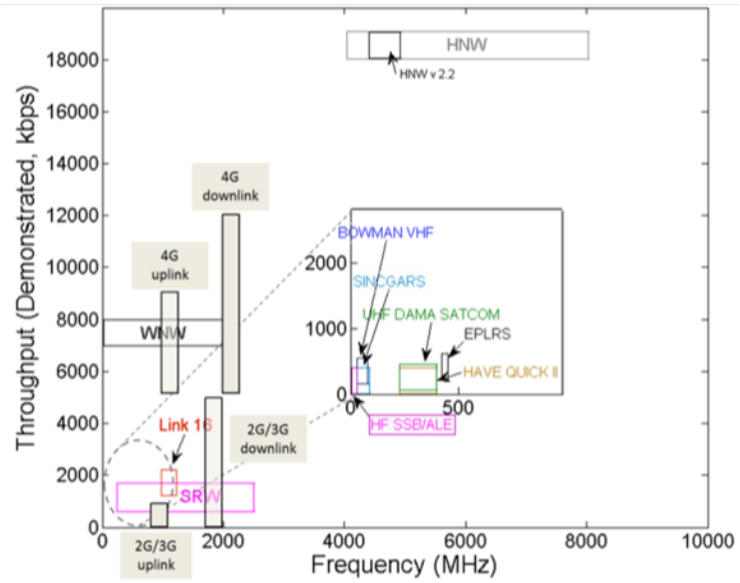

Figure 7. Military Frequency and Cellular Networks, M.S. Marwick, "Analysis of Soldier Radio Waveform Performance in Operational Test," Institute for Defense Analyses (May 2015): 64, accessed on October 31, 2019, https://apps.dtic.mil/dtic/tr/fulltext/u2/1032264.pdf.

Identify Interest, Goals, and Options

Since the post-Cold War era, and to this day, electronic warfare represents a peripheral interest to the Army. Only during the War on Terror in Afghanistan and Iraq did electronic warfare receive a brief elevation of interest to counter the enemy's use of RC-IEDs. The categorization of interests, be it vital, important, or peripheral, is a product of the funding for future capability development and acquisition. Particular to Afghanistan and Iraq, RC-IEDs represented a tactical problem with strategic consequences. Only due to the strategic implications of the RC-IED did EW receive momentary elevation to a vital interest.

In the decades before the 1991 Gulf War, the Army codified the vital interests of mobility and firepower. It pursued the "Big 5" modernization efforts focusing on the AH-64 Apache helicopter, the UH-60 Blackhawk helicopter, the M1 Abrams main battle tank, the M3 Bradley fighting vehicle, and the MIM-104 Patriot air defense system. Simultaneously, the US Navy and US Air Force focused on the electronic warfare and the Suppression of Enemy Air Defenses

(SEAD) mission. As a result, Army commanders had little experience with electronic warfare and lacked doctrine, tactics, or equipment to employ it.[40]

While the "Big 5" proved decisive during the 1991 Gulf War, the Army's reliance on electronic warfare support provided by the US Navy and US Air Force was, in part, insufficient to adapt to the complexity of the RCIEDs in Afghanistan and Iraq. By 2003, the DOD's Information Roadmap pointed out several shortfalls in electronic warfare, noting that "DoD lacks a coherent electronic warfare vision," and there exists a "disproportionate emphasis on the SEAD mission," and "there is no effective joint advocacy for planning for electronic warfare." [41] In Afghanistan and Iraq, IEDs attributed to over fifty percent of all combat casualties, of which radio triggered IEDs accounted for of over seventy percent of all IEDs. In both theaters, insurgents used a variety of techniques to detonate the bombs, including key fobs, radio-controlled toys, and other wireless technology.[42] The disproportionate focus on the electronic warfare SEAD mission proved inadequate to Army commanders confronted with RC-IEDs.

In response, the Pentagon in 2007 initiated an anti-IED task force, which became the Joint Improvised Device Defeat Organization (JIEDDO) with a budget of $4.4 billion.[43] The enemy's asymmetric techniques utilizing RC-IEDs compelled the Army to momentarily elevate electronic warfare from a peripheral to a vital interest. Technology efforts funded by JIEDDO included a range of technology efforts to include fielding over 30,000 RF jammers, each costing $60,000 to $80,000 for a total between $1.8 to $2.4 billion.[44]

---

[40] Jon M. Anderson, “The New Wizard War: Challenges and Opportunities for Electronic Warfare in the Information Age,” (2007): 6, accessed November 30, 2019, https://www.semanticscholar.org/paper/The-New-Wizard-War%3A-Challenges-and-Opportunities-in-Anderson/8a417fe01858588714a16c07a2128b861436adad.

[41] Ibid., 6.

[42] Anderson, “The New Wizard War: Challenges and Opportunities for Electronic Warfare in the Information Age,” 7.

[43] Ibid., 5.

[44] Anderson, “The New Wizard War: Challenges and Opportunities for Electronic Warfare in the Information Age,” 7.

A decade later, in 2018, the Army underwent a second modernization effort and codified the vital interests which mirror the previous "Big 5." The 2018 Army modernization effort focus was on long-range precision fires, next-generation combat vehicle, future vertical lift, Army network, air and missile defense, and soldier lethality. Despite the electronic warfare challenges experienced in Afghanistan and Iraq and the Army's pursuit of the next generation of modernization, electronic warfare is again a peripheral interest. In 2018, there are a limited number of electronic warfare systems currently fielded, and the current systems are limited to short-range dismounted and repurposed remote counter IED systems.[45]

Within the United States, frequency allocation within the electromagnetic spectrum represents an important interest. The Federal Communications Commission (FCC) retains regulatory responsibility to maintain the electromagnetic spectrum allocation between federally controlled, non-federally controlled, private, and public frequency allocations. The FCC balances competing interests of defense, private industry, and publicly available spectrum allocation. In the United States, the EMS supports a wide array of civilian infrastructure by synchronizing a wide range of computer-based systems, including law enforcement, emergency services, transportation, cellular network communications, GPS, electrical power grids, and financial transactions.[46]

Concerning our main potential adversaries of Russia and China, electronic warfare represents a vital interest with both investing in modernizing electronic warfare capabilities to disrupt or disintegrate American command and control capabilities. The multiple US conflicts the past decades provided both Russia and China an invaluable opportunity as an outside observer to learn the US strengths and identify capability gaps which to exploit. In response, both Russia and

[45] Frost, McClung, and Walls, “Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum,” 20.

[46] Westbrook, “The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare,” 1.

China invested in the modernization and integration of ground-based electronic warfare systems.[47]

The EMS supports critical civilian infrastructure. The increasing proliferation and use of cellular networks, global positioning system (GPS), and wireless technology represents a few essential examples of the civilian use of the EMS. GPS alone aids “vehicle navigation and supports critical infrastructure by synchronizing a wide range of computer-based systems including, law enforcement, emergency services, transportation, communications, electrical power grids, and financial transactions.”[48]

On the other hand, Russia and China invested heavily in modernizing electronic warfare capabilities to disrupt or disintegrate American command and control capabilities. The Russians adopted radio-electronic combat (REC) to destroy "thirty percent by jamming and thirty percent by destructive fires."[49] The Chinese developed integrated network electronic warfare (INEW), which is described as each side seeking to immobilize the other's communications, data, command, and sensor network.[50] Competing within traditional military roles of the EMS is but one fight within the electromagnetic spectrum.

The goal, given a brief understanding of the competing interests within the conceptual framework is to emphasize maximum control of the entire electromagnetic spectrum with electronic warfare. The basis for this goal follows a report from the Congressional Research Service (CRS) published in 2007 stating, "DoD now emphasizes maximum control of the entire electromagnetic spectrum, including the capability to disrupt all current and future

---

[47] Wortzel, “The Chinese People’s Liberation Army and Information Warfare,” 1.

[48] Westbrook, “The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare,” 1.

[49] Wortzel, “The Chinese People’s Liberation Army and Information Warfare,” 13.

[50] Ibid., 12.

communication systems, sensors, and weapons systems."[51] The report provides additional examples including navigation warfare where GPS is disrupted, methods to control adversary radio systems, block directed energy weapons, and lastly, to misdirect unmanned aerial vehicles (UAVs) or robots operated by adversaries.[52]

The achievement of that goal currently is in deep trouble. A source of trouble derives from the confluence of actors within the conceptual framework and competing levels of interest. In Iraq and Afghanistan, the Army enjoyed overmatch in the spectrum without substantial investment in the modernization of electronic warfare capabilities due to the threat's inability to contest US capabilities in the EMS.[53] Meanwhile, Russia and China made significant investments in modernizing and honing their electronic warfare skills and capabilities, which puts the Army at a substantial disadvantage.[54] The current mode of Army electronic warfare operations does not achieve even a limited window of tactical advantage. The Army's continued heavy reliance on devices and digital systems operating within the EMS will be our downfall if we do not recognize and work to mitigate age our vulnerabilities and our techniques for operating in a contested environment.[55]

Choosing Subject Areas for Analysis

Two options for the Army to attain the prescribed goal for maximum control of the entire electromagnetic spectrum is to pursue options for full and limited control of the EMS. Full control spans the entirety of the EMS from ELF to gamma rays on the higher end of the spectrum.

---

[51] US Library of Congress, Congressional Research Service, *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, by Clay Wilson, RL31787 (March 20, 2007), 6, accessed November 20, 2019, https://fas.org/sgp/crs/natsec/RL31787.pdf.

[52] Wilson, *Information Operations, Electronic Warfare, and Cyberwar*, 6.

[53] Frost, McClung, and Walls, "Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum," 16.

[54] Ibid., 20.

[55] Frost, McClung, and Walls, "Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum," 17.

Limited control narrows the focus to communications areas between VHF and UHF frequencies within the bands of 3-30 GHz where the majority of military operational radio communication exists.

Step 2: Performing the Analysis

The three subject areas to conduct the analysis were chosen from a provided list of twenty-five subject areas. The subject areas for analysis include; theory of action and consequence; expected effectiveness, benefits and losses; and the level of effort and resource requirements. The three subject areas chosen were most applicable to the problem, and the goal, and serves as a mechanism to explore the tradeoffs between options, the level of effectiveness for the option, and what are the required resources. Subsequently, each subject area is expanded upon in detail for each of the two purposed options.

Theory of Actions and Consequences

The theory of actions and consequences is a cause and effect analysis that evaluates the outcome and then assesses the impact of those actions. The first option for full control of the EMS represents a complex cause and effect relationship that requires multiple changes that are challenging to overcome in the short term. The option is complex due to the number of competing interests and existing regulatory control of the EMS domestically and internationally. To exercise full control requires reform to existing domestic and international law regarding the regulation of the EMS. Within the United States, spectrum management is divided among two agencies: the FCC for the private and state and local governments, and the NTIA for federal government users. Internationally, the United Nations International Telecommunications Union (ITU) manages radio regulation through bilateral and multilateral agreements which the Department of State is the lead department for international spectrum use. The modification to existing EMS policies is a multi-level negotiation to achieve domestic and international consensus. Ultimately, option one is

difficult to realize because the Army or even DoD is not the lead department for the negotiation of such policies to enable maximum control of the EMS.

The second option for limited control represents a complicated cause and effect relationship because it operates within existing domestic and international agreements and limits the range of required electronic warfare capabilities. The cause and effect relationship for the second option remains complicated because domestic and international EMS management does not always align. A system approved for use by the Army is subject to approval by the host country and may generate electromagnetic interference (EMI) when operating as a coalition member.

Expected Effectiveness, Benefits, and Losses

The second area of analysis builds upon the cause and effect relationship of the first area of analysis to determine the effectiveness, benefits, and losses. The first option of total control is appealing due to the expected benefit but is disproportional considering the holistic cost-benefit. The rationale for full control implies that if the Army controls EMS for its use then by result can deny its use by the adversary. Developing capabilities across the EMS ensures the breadth of coverage but may lack sufficient depth in any one particular area to ensure effectiveness. Additionally, the pursuit of control of the entirety of the EMS is unrealistic because only a portion of the EMS is used for communications purposes. The option of developing capabilities across the EMS outside of communication purposes introduces additional requirements that are already marginally succeeding. For that reasoning, the expected gains to control the breadth of the EMS does not exceed the anticipated losses in depth of the primary communication bands.

The second option for limited control of the EMS ensures depth focused on the primary communication bands (UHF, VHF) within the EMS. Focusing efforts toward limited control within the UHF and VHF parameters provides the highest degree of effectiveness to achieve the goal. Focusing control to the UHF and VHF communication bands affords the Army a predictive funding estimate and ability to consistently fund other priorities. Inherently, the negative

consequence is the acceptance that the Army is not effective outside areas of limited control. The impact of the negative consequence is overcome by the reduced likelihood and severity of not developing capabilities outside those regions. The civilian sector, the Army, and our adversaries all compete for communication dominance in the UHF and VHF regions of the EMS.

Level of Effort and Resource Requirements, and Cost

The level of effort, resource requirements, and costs is the third method for analysis between total control and limited control of the EMS. The first option for total control of the EMS is a significant endeavor in terms of resource requirements and cost. The endeavor is significant due to the nature of the EMS from ranging from ELF on the lower end to gamma rays on the higher end. The next step for the Army is to then develop technology and capabilities to control those emissions across the spectrum. Currently, the EMS is loosely compartmentalized across the Joint Force with the US Navy utilizing low-frequency bands on nuclear-armed submarines to communicate with national command authority and the US Air Force utilizing extremely high-frequency bands to communicate with US satellite constellations. The compartmentalization of the radio spectrum maximizes capabilities and shares the cost burden of developing technology to serve their respective services. To pursue total control of the EMS, the Army would incur significant additional costs once shared by other services at the detriment of other capabilities and programs. The costs associated with total control of the EMS are not easily bearable to the Army and too expensive to contemplate. Total control of the EMS is loosely associated with only one of six of the 2018 modernization efforts. The option for total control of the EMS potentially risks the disruption of the remaining five priorities. The five remaining programs focus on mobility and lethality are vital interests to land warfare which is the core mission of the Army.

The second option for limited control of the EMS represents a significant level of effort, resources requirements, and costs associated. The significant level of effort required derives from the requirement to change the operating paradigm of the Army is in jeopardy, short of a moment of crisis. The option for limited control of the EMS is starting anew due to the decades of the

divestiture of electronic warfare capabilities as a cost-saving measure to fund emergent high priority requirements. To overcome obsolete equipment and lost expertise the Army faces significant resource requirements and costs. The long-term costs and resource requirements for limited control of the EMS are bearable for the Army in terms of investment in technology, personnel, and training.

Recommendations

The recommendation based upon the analysis is for the Army to pursue capabilities to enable limited control of the electromagnetic environment. Currently, limited control of the electromagnetic spectrum exceeds current capabilities because of the human in the loop interaction. Current electromagnetic spectrum operations rely on human interaction to allocate and deconflict the electromagnetic spectrum and for the end-user to adhere to the set control measures.[56] In the event, the end-user does not comply with the control measures introduced, the risks of electromagnetic interference increases. Given the increasingly complex nature and saturation of the electromagnetic spectrum by the civilian sector, the military, and the adversary with the human in the loop, existing procedures are inadequate to account for the speed and dynamic nature of the electromagnetic environment. Figure 8 below provides a graphical depiction of the task for electromagnetic spectrum mangers to rapidly integrate, synchronize, and deconflict the electromagnetic spectrum.

[56] Department of the Army, Field Manuel (FM) 3-12, *Cyberspace and Electronic Warfare Operations Fundamentals* (Washington, DC: Government Printing Office, April 11, 2017), 1-35.

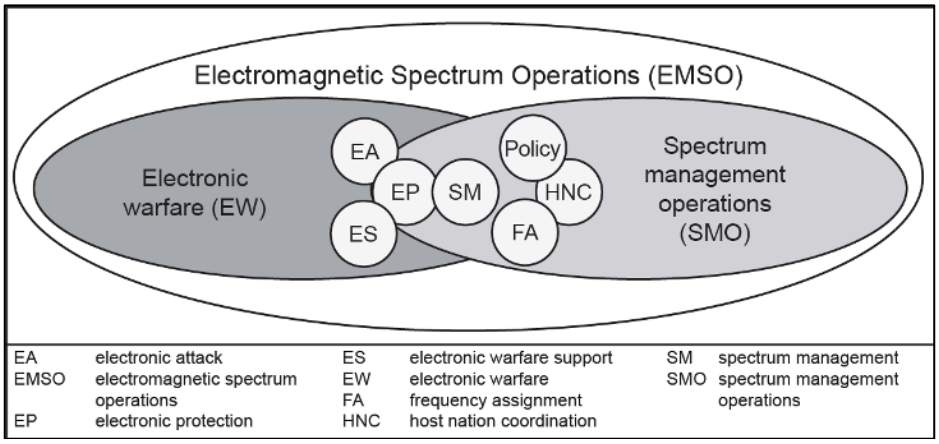

Figure 8. Electromagnetic Spectrum Operations, US Department of the Army, Field Manuel (FM) 3-12, *Cyberspace and Electronic Warfare Operations Fundamentals* (Washington, DC: Government Printing Office, 2017), 1-34.

What Figure 8 does not depict is a mechanism to rapidly conduct these actions iteratively as the civilians, the military, and the adversary compete within the electromagnetic spectrum. The key take-away from Figure 8 is that the Army is sometimes its own worst enemy.

The introduction of artificial intelligence and machine learning to electromagnetic spectrum management provides a capability to increase situational awareness and rapidly adapt to changes within the electromagnetic spectrum. Machine learning is an application of artificial intelligence that provides systems the ability to learn and improve from experience without being explicitly programmed automatically. Spectrum management is the operational, engineering, and administrative procedures to plan, coordinate, and manage the use of the electromagnetic spectrum and enables signal and electronic warfare operations.[57]

The purpose of artificial intelligence and machine learning in this context is to identify civilian, military, and adversarial signal patterns, filter unwanted signals, provide a graphical user interface of the electromagnetic spectrum, adjust the friendly frequency allocation to less congested frequency bands. Figure 9 below provides a graphical representation of the fusing of disparate data sources from the host nation, adversarial signals, and friendly spectrum allocations with electronic attack and electronic protect frequencies.

[57] US Army, FM 3-12, 1-34.

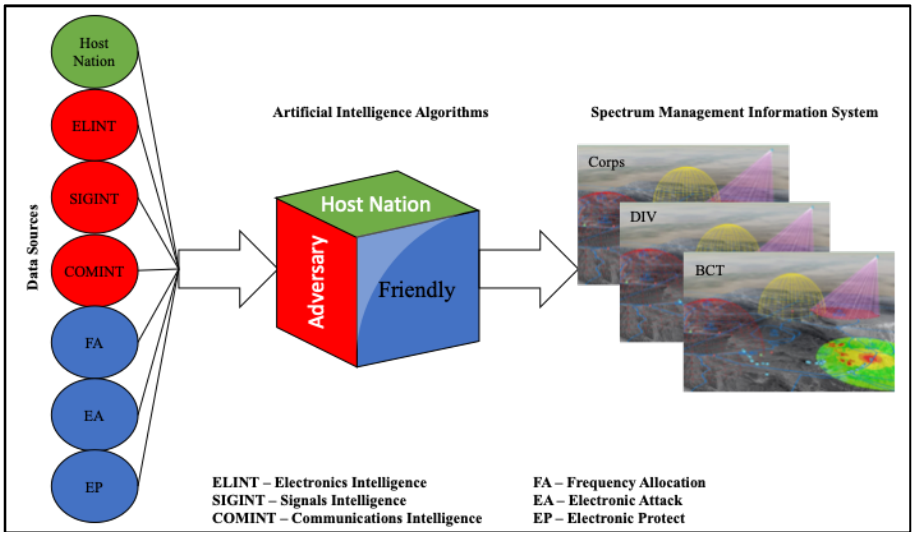

Figure 9. Artificial Intelligence Enabled Electromagnetic Spectrum Operations.

Artificial intelligence and machine learning utilizes algorithms to fuse the data sources and then graphically portrays the electromagnetic spectrum on a usable graphical user interface. The development and use of artificial intelligence and machine learning increases the rate of adaptability of electromagnetic spectrum operations considering the dynamic nature of the electromagnetic environment.

As a first step, the Army is in the initial development and fielding of the electronic warfare planning and management tool (EWPMT). The EWMPT system provides enhanced situation awareness of the electromagnetic environment, identify adversary signals, which equips forces with essential electronic warfare mission-planning capabilities. The EWPMT main capability which the EWPMT provides the Army is the ability to sense and characterize the EMS (civilian sector, military, or the adversary.) Ideally, prior to the initiation of military operations an EW baseline occurs to characterize and determine the volume of signals within the AO. Once an EW baseline occurs staffs are able to identify potential anomalies and characterize as either friendly or adversary transmission sources. As EWPMT technology continues to develop future capability sets offer the ability for real-time collaborative management of the electromagnetic spectrum and inter-echelon communication. What that means is the ability for the EWPMT to sense the EMS and identify high and low usage radio bands and to then transition radio

communications to lower use or available frequency bands to minimize EMS fratricide and improve communications reliability.

The use and development of artificial intelligence and machine learning is not meant to portray a panacea "black box" to cure all the Army's aliments. What it does provide is a first step to sense the electromagnetic environment and convert what is invisible to the naked eye to a tangible visual representation of the electromagnetic spectrum battlespace. Additionally, developing an artificial intelligence capability then provides a baseline to develop and integrate future electronic warfare specialists and electronic warfare equipment to further optimize the Army's electronic warfare capabilities.

Conclusion

Prior to initiating this endeavor, the research question postulated how does the Army control a contested electromagnetic spectrum to enable operational maneuver? The hypothesis stated that the Army develops a policy for electronic warfare that seeks to control the entirety of the electromagnetic spectrum. The policy comprises both materiel and non-materiel capability-based approaches which are necessary to dominate the electromagnetic spectrum in future warfare.

To pursue those aims, the research methodology utilized Richard Kugler's two-step methodology for analyzing policy options for a single goal. The single goal sought maximum control of the entire electromagnetic spectrum, including the capability to disrupt all current and future communication systems, sensors, and weapons systems. The two options analyzed were full or partial control of the electromagnetic spectrum. The subject areas for analyzed included; theory of action and consequence; expected effectiveness, benefits, and losses; and the level of effort and resource requirements. The four subject areas of analysis are most applicable to the research question and hypothesis.

Through the course of research and analysis, the initial hypothesis proved only partially correct. Ultimately, the Army is best served to pursue limited control of the electromagnetic with full control infeasible due to interest, costs, and infeasibility to control the entirety of the electromagnetic spectrum all the time. Secondly, the recommendation focused on non-materiel solutions with the utilization of artificial intelligence and machine learning to enable electromagnetic spectrum operations. The focus on non-materiel solutions is vital because it seeks to fuse traditional electromagnetic spectrum operations, intelligence, and electronic warfare to prevent electromagnetic interference. Ultimately, artificial intelligence and machine learning applied to the electromagnetic spectrum operations provides a capability for the Army to enhanced situational awareness to enable periods of overmatch in the conduct of multi-domain operations.

The area not addressed in this endeavor is the materiel aspects of electronic warfare equipment required to support multi-domain operations. Currently, the Army is equipped with only residual ground-based electronic warfare equipment repurposed for the C-IED threats during operations in Afghanistan and Iraq. Comparatively, the Army's electronic warfare equipment is outnumbered and outmatch by adversaries such as Russia and China. Despite a short-term disadvantage a long-term opportunity exists, if acted upon in the near term. To seize the advantage, the Army potentially achieves a generational leap by fielding advanced electronic warfare systems instead of incremental improvements of legacy systems. If the Army pursues this option, the adversarial systems would instantly become obsolete in relation to the capability of US electronic warfare systems.

To conclude, the keystone to conduct multi-domain operations across the range of military operations in large-scale combat operations is electromagnetic spectrum operations enabled through the use of artificial intelligence and machine learning.

Bibliography

Darnton, G. “Information Warfare, Revolutions in Military Affairs, and International Law.” *Journal of Information Warfare* 4, no. 1 (2005): 1-20. Accessed September 26, 2019. https://jstor.org/stable/10.2307/26504013.

Ebbut, Giles, Michael J. Gething, and John Williamson. *IHN Janes’s C4ISR & Mission Systems: Joint & Common Equipment*. IHS, 2013.

Frost, Patricia, Clifton McClung, and Christopher Walls. “Tactical Considerations for a Commander to Fight and Win in the Electromagnetic Spectrum.” *The Cyber Defense Review* 3, no. 1 (2018): 15-26. Accessed September 21, 2019. https://www.jstor.org/stable/10.2307/26427371.

Gherman, Laurian. “Electronic Warfare in Information Age.” *Review of the Air Force Academy* 27, no. 3 (2014).

Huber, Arthur F., Gary Carlberg, Prince Gilliard, and L. David Marquet. “Deconflicting Electronic Warfare in Joint Operations.” *Joint Force Quarterly* 42 (2007): 89-95. Accessed November 20, 2019. https://pdfs.semanticscholar.org/9c86/2ecff750d66c2b2f654b87e0b3066e1b4ea9.pdf?_ga=2.99443422.11420435.1567623667-1872443529.1567623667.

Kugler, Richard. *Policy Analysis in National Security Affairs: New Methods for a New Era*. Washington, DC: National Defense University Press, 2006.

Maini, Anil K. *Handbook of Defence Electronics and Optronics: Fundamentals, Technology and Systems.* New York, NY: John Wiley & Sons, 2018.

Milian, Mark. “U.S. Government, Military to get Secure Android Phones." CNN, February 3, 2012. Accessed September 26, 2019. http://edition.cnn.com/2012/02/03/tech/mobile/government-androidphones/index.html?eref=rss_mostpopular.

Munro, Neil. *The Quick and the Dead*. New York: St. Martin’s Press, 1991.

Niekerk, Brett and M. Maharaj. “The Future Roles of Electronic Warfare in the Information Warfare Spectrum.” *Journal of Information Warfare* 8, no. 3 (2009): 1-13. Accessed September 2, 2019. https://www.jstor.org/stable/10.230726486763.

Niekerk, Brett. “Mobile Devices and the Military: Useful Tool or Significant Threat?” *Journal of Information Warfare* 11, no 2 (2012): 1-11. Accessed September 26, 2019. https://www.jstor.org/stable/10.2307/26486774.

O’Connor, Marc. “Electronic Warfare for the Fourth Generation Practitioner.” *Small Wars Journal*. Accessed November 29, 2019. https://smallwarsjournal.com/jrnl/art/electronic-warfare-fourth-generation-practitioner.

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

Pye, Gillian and M.J. Warren. “An Emergent Security Risk: Critical Infrastructures and Information Warfare” *Journal of Information Warfare* 8, no. 3 (2009): 14-26. Accessed November 20, 2019. https://www.jstor.org/stable/10.2308/26486764.

Pye, Gillian and M. Maharaj. “The Future Roles of Electronic Warfare in the Information Warfare Spectrum” *Journal of Information Warfare* 8, no. 3 (2009. Accessed November 20, 2019. https://www.jstor.org/stable/10.2307/26486763.

Richardson, Doug. *An Illustrated Guide to the Techniques and Equipment of Electronic Warfare*. New York: Arco Publishing Inc. 1985.

Schleher, D. Curtis. *Electronic Warfare in the Information Age*. Boston, MA: Artech House, 1999.

US Department of the Army. “Army Modernization Strategy: Investing in the Future, 2019.” Accessed on November 10, 2019. https://www.army.mil/e2/downloads/rv7/2019_army_modernization_strategy_final.pdf.

US Department of the Army. Army Techniques Publication (ATP) 6-02.53, *Techniques for Tactical Radio Operations.* Washington, DC: Government Printing Office, 2016.

US Department of the Army. Field Manuel (FM) 3-12. *Cyberspace and Electronic Warfare Operations Fundamentals.* Washington, DC: Government Printing Office, 2017.

US Department of the Army. TRADOC Pamphlet (TP) 525-3-1. *The U.S. Army in Multi-Domain Operations 2028.* Washington, DC: Government Printing Office, 2018.

US Department of Defense. “Electromagnetic Spectrum Strategy 2013: A Call to Action.” Accessed December 26, 2019. https://dodcio.defense.gov/Portals/0/Documents/Spectrum/ESS.pdf.

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

US Library of Congress. Congressional Research Service. *Convergence of Cyberspace Operations and Electronic Warfare*, by John R. Hoehn and Catherine A. Theohary, IF11292. August 13, 2019. Accessed January 29, 2020. https://fas.org/sgp/crs/natsec/IF11292.pdf.

US Library of Congress. Congressional Research Service. *Defense Primer: Electronic Warfare*, by John R. Hoehn. IF11155. September 18, 2019. Accessed November 10, 2019. https://fas.org/sgp/crs/natsec/IF11118.pdf.

US Library of Congress. Congressional Research Service. *Defense Primer: Military Use of the Electromagnetic Spectrum*, by John R. Hoehn. IF11155. May 24, 2019. Accessed January 28, 2020. https://fas.org/sgp/crs/natsec/IF11155.pdf.

US Library of Congress. Congressional Research Service. *Information Operations, Electronic Warfare, and Cyberwar: Capabilities and Related Policy Issues*, by Clay Wilson. RL31787. March 20, 2007. Accessed November 20, 2019. https://fas.org/sgp/crs/natsec/RL31787.pdf.

Vakin, Sergei A., Lev N. Shustov, and Robert H. Dunwell. *Fundamentals of Electronic Warfare*. Boston: Artech House, 2001.

Westbrook, Tegg. "The Global Positioning System and Military Jamming: The Geographies of Electronic Warfare." *Journal of Strategic Security* 12, no. 2 (2019): 1-16. Accessed September 15, 2019. https://www.jstor.org/stable/10.2307/26696257.

Wortzel, Larry M. "The Chinese People's Liberation Army and Information Warfare." *Strategic Studies Institute* (2014). Accessed September 15, 2019. http://www.jstor.org/stable/resrep11757.