Electronic Warfare and Organizational Encopresis: The Neglect of the US Army and Its Intelligence Branch to Advocate for Warfighting Capabilities in the Electromagnetic Spectrum

A Monograph

by

MAJ Kenneth T. King
US Army

MENS EST CLAVIS VICTORIAE

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

2019

REPORT DOCUMENTATION PAGE

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

4. TITLE AND SUBTITLE Electronic Warfare and Organizational Encopresis: The Neglect of the US Army and its Intelligence Branch to Advocate for Warfighting Capabilities in the Electromagnetic Spectrum	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) MAJ Kenneth T. King	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 Ft. 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 is unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This monograph focuses on stunted development of the US Army's modern electronic warfare (EW) capability. It compares the technological change that occurred in the US Army, Air Force, and Marines as it relates to the electromagnetic spectrum. It explores how the Army's Intelligence Branch, which was the proponent of the EW discipline from 1955 to 2005, mismanaged the discipline. Additionally, this monograph evaluates the Army's different operational concepts and the degree to which they advanced or retarded EW capacities. The US Army and Intelligence Branch involuntary and intentionally neglected EW at different times throughout the history of the capability. A situation, from which the psychological disorder of encopresis is a metaphor. The US Army is still neglecting the EW discipline as of the writing of this monograph even as its competitors continue to advance its EW technology and tactics.

15. SUBJECT TERMS
Electronic Warfare, Intelligence Branch, Army Security Agency, Trafficjam, Quickfix, signals intelligence, F-111 Raven, EC-130 Compass Call, CREW Vehicle Receiver Jammer, CREW Duke, Prophet

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

Monograph Approval Page

Name of Candidate: Kenneth T. King, Major

Monograph Title: Electronic Warfare and Organizational Encopresis: The Neglect of the US Army and Its Intelligence Branch to Advocate for Warfighting Capabilities in the Electromagnetic Spectrum

Approved by:

_____, Monograph Director
John M. Curatola, PhD

_____, Seminar Leader
Heiko Diehl, COL

_____, Director, School of Advanced Military Studies
Kirk C. Dorr, COL

Accepted this 23rd day of May 2019 by:

_____, Director, Graduate Degree Programs
Robert F. Baumann, PhD

Abstract

Electronic Warfare and Organizational Encopresis: The Neglect of the US Army and Its Intelligence Branch to Advocate for Warfighting Capabilities in the Electromagnetic Spectrum, by MAJ Kenneth T. King, 48 pages.

This monograph focuses on stunted development of the US Army's modern electronic warfare (EW) capability. It compares the technological change that occurred in the US Army, Air Force, and Marines as it relates to the electromagnetic spectrum. It explores how the Army's Intelligence Branch, which was the proponent of the EW discipline from 1955 to 2005, mismanaged the discipline. Additionally, this monograph evaluates the Army's different operational concepts and the degree to which they advanced or retarded EW capacities. The US Army and Intelligence Branch involuntary and intentionally neglected EW at different times throughout the history of the capability. A situation, from which the psychological disorder of encopresis is a metaphor. The US Army is still neglecting the EW discipline as of the writing of this monograph even as its competitors continue to advance its EW technology and tactics.

Acknowledgements

Contents

Illustrations

Acronyms

ASA	Army Security Agency
CEWI	Combat Electronic Warfare and Intelligence
CREW	Counter Radio-controlled Improvised Explosive Device Electronic Warfare
EA	Electronic Attack
EW	Electronic Warfare
IED	Improvised Explosive Device
INSCOM	Intelligence and Security Command
MI	Military Intelligence
SIGINT	Signals Intelligence
TRADOC	Training and Doctrine Command
US	United States
USSR	United Soviet Socialist Republic

Introduction to Electronic Warfare

The United States (US) is losing the fight for the electromagnetic spectrum. Our adversaries have made advances in its concepts and technology while the US Army has not. The former chief of electronic warfare (EW) for the Army, Colonel (Retired) Jeffrey Church, is on record describing the problem. He claims the Russians and Chinese have "spent the last 20 years continuing the development and acquisition of an electronic warfare capability, whereas . . . the Army got out of the business."[1] EW, warfare between electronic emissions on the battlefield, is a lost art the Army must recover to remain competitive. But before the Army can reclaim this art form, it is crucial to assess the lessons which led to EW's obsolescence. We must critically consider who was responsible for the decline of EW and why. That way, the same factors that doomed it before do not appear again in its reintroduction.

To the question of who is responsible, the answer seems to be the Intelligence Branch of the US Army. Comparing the branch's relationship with EW in the past to more recent efforts of integration, Colonel Church lamented that if EW is once again placed under the Intelligence Branch, "the intel people will finally be able to get rid of EW, again, by taking it over, again, and crushing it."[2] While this may be slight hyperbole, there is truth to Colonel Church's claim. The Intelligence Branch has been the proponent of EW since 1955 and still retains parts of the discipline.[3] The story of EW is an arc which gains momentum through the 1980s as the Army formed EW units and fielded new EW technology. EW reached its zenith in the Combat Electronic Warfare Intelligence (CEWI) battalions and brigades in the 1980s. These units

---

[1] Morgan Chalfant, "Army Struggling to Fund Projects to Combat Electronic Warfare," *The Washington Free Beacon*, July 20, 2015, accessed January 24, 2019, https://freebeacon.com/national-security/army-struggling-to-fund-projects-to-combat-electronic-warfare/.

[2] Sydney J. Freedberg Jr., "Army Wrestles with SIGINT vs. EW," *Breaking Defense*, July 31, 2018, accessed January 24, 2019, https://breakingdefense.com/2018/07/army-wrestles-with-sigint-vs-ew/.

[3] John Patrick Finnegan and Romana Danysh, *Military Intelligence* (Washington, DC: Center of Military History, 1998), 167.

supported the Army's divisions and corps with varied EW and intelligence soldiers.[4] CEWI organizations and EW technologies atrophied through the 1990s due to budget and troop cuts. Operations Iraqi Freedom and Enduring Freedom shifted the focus away from EW use on a conventional battlefield. Based only on this chronology, it seems the Intelligence Branch let EW wither during this period. So much so that by 2005, the proponent of EW became the Fires Branch. However, it was not through willful neglect that the branch placed EW on the backburner. The Army's shifting doctrinal focus from the 1970s through the present day also caused the decline. The story of EW is vital to the future, as soldiers attempt to rebuild this capability; but merely fixing blame and approximating the cause is not enough. The Army must attempt to recover EW capability to remain competitive with its adversaries.

This monograph will attempt to explain how the Intelligence Branch, due to internal biases, and how the Army, through institutional ignorance, neglected the nation's EW capacity. The Army focused on EW in the 1970s as a part of the doctrine of "Active Defense." The Intelligence Branch maintained this focus despite changes in warfighting concepts and technological advances in EW. In some cases, however, the branch used the EW moniker to gain support for funding, without actually placing EW in the same standing as other disciplines, such as signals intelligence (SIGINT). The Global War on Terrorism reset ideas about EW within the conduct of counterinsurgency. These events shifted the focus of the Army away from EW-specific platforms. The branch, unable to provide a viable path for EW, ceded the discipline to the Fires Branch.

A major storyline of the branch's neglect of EW lies in the complications and biases towards SIGINT. SIGINT, with its regulatory ties to the National Security Agency, made integration at the corps, division, and brigade echelons difficult for EW. The deputy chief of

---

[4] Michael Bigelow, "Short History of Army Intelligence," *Military Intelligence Professional Bulletin* 34-12–3 (September 2012): 59.

Army staff for intelligence, Lieutenant General Scott Berrier, acknowledges this difficulty. He noted the primary challenge of EW "is one of integration . . . [that] . . . future forces must integrate SIGINT, electronic warfare, and cyber capabilities to provide situational awareness."[5] These ideas are complementrary and have been combined in the same technologies and organizations in the past, however with limited success.

This monograph is also concerned with how the Army compensated for reduced EW by assuming Air Force coverage in the next war. Given the atrophy of ground-based EW since the mid-1970s, the Army relied on the other services' EW assets. The Air Force and Marines (as part of the Navy) always included EW warfare, focused on radar jamming, in their competences; so, in some cases, it makes sense for the Army to outsource its EW requirements. Many issues with ground-based EW revealed themselves in the Gulf War. The Air Force conducted EW during that war extensively, but ground-based EW in only a limited fashion. Instead of trying to address problems, the Army doubled down on Air Force EW, letting ground-based systems atrophy. The problem today is that there are too few aircraft with a dedicated EW mission. There are even fewer that will likely support the Army in the next war.

Lastly, this monograph will explore the role of the Army Security Agency (ASA), previously the Army's SIGINT branch, in undermining the EW discipline. The role of the ASA is tragic because it provided EW its best hope for survival but played a leading role in its demise. The ASA had enough independence and power within the Army's bureaucracy to actually innovate EW. The problem, however is that it did not. The ASA became overly focused on its core competencies instead of a more long-term approach which also focused on EW development.

---

[5] Freedberg, "Army Wrestles with SIGINT vs. EW."

When referring to EW, there are three divisions which must be defined. The first is EW support, which involves the interception, identification, and location of electromagnetic activity.[6] Second is electronic attack (EA) which are actions taken within the electromagnetic spectrum to affect an enemy's combat power deliberately. These actions will "prevent or reduce the enemy's effective use of the electromagnetic spectrum" to include jamming, disruption, and deception.[7] Last, electronic protection is the passive and active means to "protect personnel, facilities, and equipment from . . . EW."[8] These three divisions taken together are the breadth of EW functions within the Army.

This monograph focuses on non-technical aspects of EW to maintain permissive classification. It focuses on the relation of EW, the Intelligence Branch, and the Army as it relates to technologies, organization, and doctrine. It will take short forays into other related topics, such as EW in other services and SIGINT's parent organizations. The work remains bounded between 1955, when the Intelligence Branch gained proponency of EW, through the present. Its chronological emphasis, however, is on the advent of modern EW after the 1973 Arab-Israeli War through 2005 when the Fires Branch acquired parts of the EW discipline.

The emphasis of this monograph is the relationship between EW, the Intelligence Branch, and US Army doctrinal concepts; it does not presume to advocate complete solutions. There are several conclusions in this paper that hint at a possible course of action for EW in the future. However, the author does not have the requisite experience in EW technology or the larger aspects of the discipline outside the scope of this paper. Thus, the following analysis remains a viewpoint about the lack of contemporary EW efficacy and the argument that it was induced by

---

[6] US Department of the Army, *Army Doctrinal Reference Publication (ADRP) 1-02, Operational Terms and Graphics* (Washington, DC: Government Printing Office, 2016), 1-33.

[7] Don E. Gordon, *Electronic Warfare: Element of Strategy and Multiplier of Combat Power*, 2nd ed. (Oxford: Pergamon, 2014), 5.

[8] US Army, *ADRP 1-02* (2016), 1-33.

the organizations which were supposed to be its advocates. Larger questions of future positive roles of US Army EW must be left to the practitioners within that discipline who understand the technology and those located within the bureaucracy who understand the dynamics of EW within the larger US defense concept.

Electronic Warfare Technology

In 1988, when the AN/TLQ-17 "Trafficjam" EW platform was fielded, it weighed more than 10,000 pounds. The Trafficjam was the preeminent EW jammer on the modern battlefield until removed from service in the early 2000s. The EW platform most widely used by the Army in 2019 is the AN/VLQ-12 Counter Radio-controlled Improvised Explosive Device Electronic Warfare (CREW) Duke system which weighs 69 pounds.[9] The difference in hardware, software, transport, and the role of the two could not be more different. Their comparison is a metaphor for the advancement of EW within the US Military. The advancement of technology has been a fundamental driver of this change in the EW discipline. The Intelligence Branch, the Army's proponent for EW, was instrumental in the development of both these and preceding technologies. While the Trafficjam was one of the branch's most significant projects, the CREW Duke was completely reactionary. The Army developed a paradigm for useful jamming technology that was not questioned by the discipline's proponent. Unlike the Air Force, the Army failed to prioritize EW acquisition and was deficient in recognizing technological trends across services.

The Army, Air Force, and Marines have generally followed the same trajectory of EW technology but each at its own pace. The three services have moved from dedicated EW weapons

---

[9] John Pike, "AN/TLQ-17A(V), TRAFFICJAM," Federation of American Scientists, January 21, 1999, accessed January 19, 2019, https://fas.org/man/dod-101/sys/land/an-tlq-17.htm; "CVRJ CREW Fact Sheet," Marine Corps System Command, accessed January 19, 2019, https://www.marcorsyscom.marines.mil/Portals/105/PMMC3/MC3PDF/2%201%20CVRJ%20CREW%20FACT%20SHEET.pdf.

to fitting various platforms within its inventory with EW technology. The move from the Air Force's EF-111 "Raven," used extensively during the 1990s, to the F-16 and F-35, in which EW packages were standard, are prime examples. Current interest in electronic counter-measures has democratized EW and deemphasized the traditional focus, EA.[10] For different reasons, but related to constraints of technology, the Air Force, Army, and Marines have settled on similar deployment methods for EW. All three services have proliferated less capable EW technology across a multitude of platforms. This chapter will briefly review the programs of each service, comparing and contrasting EW capability.

The Army, specifically, failed to keep pace with the Air Force in developing its EW platforms and concepts. Organizational constraints related to the lack of focus on the development of EW technology was a major contributor to this lag. The Army, in allowing the Intelligence Branch to dictate the future of the discipline, ensured it would not receive dedicated resources and development. The branch focused on its core intelligence gathering capabilities. Maintenance of EW within the ASA, traditionally the most secretive element of the Intelligence Branch with significant restrictive classifications related to enemy communications, exacerbated the problem. [11] Another factor was the difference in targets of the Air Force and Army. The ladder was more focused on communications which significantly advanced from the 1970s to the present day. The Air Force, on the other hand, was more concerned with jamming radars, a more tangible military-specific problem, in juxtaposition to the US Army's need to interdict communications equipment.[12] The rate of change in communications technology forced the Army to rely on commercial off-the-shelf equipment. This history of the Army's EW program is an important

---

[10] "F-16 Fighting Falcon Multirole Fighter," Air Force Technology, accessed January 20, 2019, https://www.airforce-technology.com/projects/f16/; "F-35 Electronic Warfare Capabilities," Lockheed Martin, accessed January 20, 2019, https://www.f35.com/about/capabilities/electronicwarfare.

[11] Finnegan and Danysh, *Military Intelligence,* 180-81.

[12] Alfred Price, *The History of US Electronic Warfare, Volume 3, Rolling Thunder Through Allied Force, 1964-2000* (Alexandria, VA: Association of Old Crows, 2000), 226.

departure point to understand how the discipline evolved in the various services. It specifically highlights the delinquencies of the Intelligence Branch in its maintenance.

Early Army Electronic Warfare Technology

Ground-based EW is constrained by terrain and technology, both of which the Army was able to compensate for by the 1980s, but not without difficulty. The constraints on EW technology are related to considerations of line-of-sight and power. The ability to jam radio signals is a function of power output against an opposing communications signal. Where the signal from the EW platform is greater than the signal, jamming will occur. Additionally, greater power is required when an opposing communications signal is farther away. For jamming to occur, the two signals have to be spatially contiguous, i.e. line-of-sight between the two platforms is required.[13] Figure 1, from the 1987 version of Field Manual 34-1, *Intelligence and Electronic Warfare Operations* demonstrates the varying considerations of distance and line-of-sight.

---

[13] Michael R. Frater and M. J. Ryan, *Electronic Warfare for the Digitized Battlefield* (Norwood, MA: Artech House, 2001), 145-146.
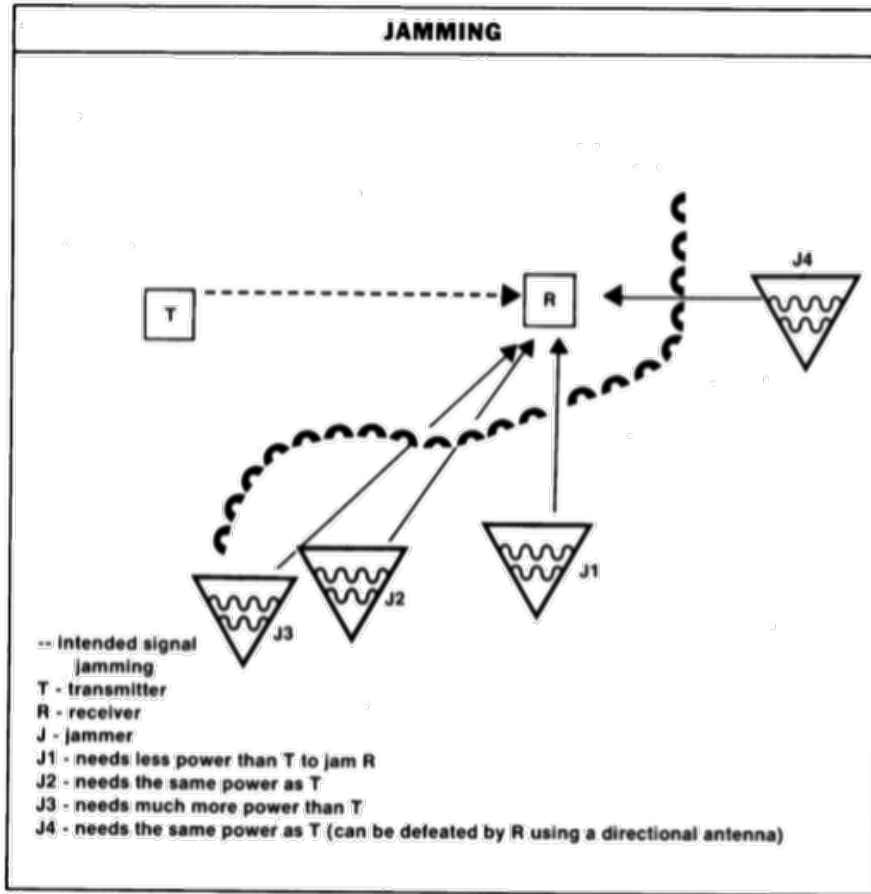
Figure 1.   Jamming Considerations
Source: US Department of the Army, Field Manual (FM 34-1), *Intelligence and Electronic Warfare Operations* (Washington, DC: Government Printing Office, 1987), 5-3.

Power was the crux of the problem for aerial jamming, integrating power sources small enough to fit on planes with enough power to project a jamming signal. For the Air Force, this was primarily a math problem, waiting for technology to develop solutions. More so, the Army has to consider enemy capabilities in developing its EW technology. Electromagnetic capabilities are, for all significant purposes, direct fire weapons; thus, ground-based jammers will often be within range of enemy indirect fire artillery.[14] Due to this and the large jamming signal emitted,

---

[14] Army Intelligence Center, *Student Text 2-50, Intelligence and Electronic Warfare (IEW) Systems* (Fort Huachuca, AZ: Army Intelligence Center, 2002), 23.

EW assets are often perilously vulnerable. So, the Army had a myriad of problems with which the Air Force did not need to contend.

While the Air Force's airplanes are innately mobile, constraints of the terrain often required the Army's ground-based EW platforms to conduct jamming at a halt. This constraint made them vulnerable.[15] The ability to remain mobile rested on factors of size, weight, and power (often noted by the acronym SWaP).[16] EW technology had to be small enough and weigh only as much as could be transported on a military prime mover, but it also had to be attached to enough power to project a jamming signal over a significant range.

The progression of this concept is illustrated in the transition from fixed radio communication sites to the mobile truck-mounted EW solutions. The first recorded example of EW was during the Russo-Japanese War of 1904. The Russians, from their large fixed site in Port Arthur, were able to jam communications between two Japanese navy ships. The fixed site was able to overpower the weaker naval signal. In this instance, Russian efforts led to the withdrawal of the ships and a respite from naval bombardment on the port.[17] As the commercial sector developed hardware that was smaller and lighter while maintaining similar signal strength, EW platforms became viable on the modern battlefield.

The Army was able to field its first EW platforms by the 1980s but not without considerable difficulty and questionable success. The AN/TLQ-17 "Trafficjam" was the Army's answer to overcoming the physical constraints associated with ground-based EW. Technology had made size and power requirements manageable, but only to a point. The Trafficjam was still

---

[15] Frater and Ryan, *Electronic Warfare for the Digitized Battlefield*, 121-125.

[16] John Keller, "SWaP: How Size, Weight, and Power Are Transforming the Military Electronics Industry," *Military and Aerospace*, June 1, 2013, accessed January 20, 2019, https://www.military aerospace.com/articles/print/volume-24/issue-6/news/trends/swap--how-size--weight--and-power-are-transforming-the-military-.html.

[17] Frater and Ryan, *Electronic Warfare for the Digitized Battlefield*, 121-125.

limited by the terrain features which would "mask" the emission from its small antenna.[18] The

mobility required within tactical forces limited the power the Trafficjam could emit. All of these

issues with ground-based mobile EW platforms were prevalent during the United States'

Operation Desert Storm.[19] In theory, problems with ground-based EW were somewhat absolved

by the Army's AN/ALQ-151 "Quickfix" Helicopter. While power was still a problem, the ability

to fly above terrain features while maintaining mobility made the platform effective. However,

the dozen Quickfix which deployed during the 1990 Gulf War had limited success due to Iraqi

communications security.[20]

The bigger problem for ground-based EW was the rate of technological change in

communications systems. In an attempt to advance its systems, the Army re-developed the

Quickfix as the Advanced Quickfix and the TLQ-17. However, the Army fielded neither system

because its acquisition process was not progressive enough. It could not account for changes in

enemy technology and an increasingly complex battlefield.[21] But shortly after, the concept for the

"Prophet" System was initiated. The Prophet was supposed to incorporate SIGINT and EA

capabilities into one system.

---

[18] US Department of the Army, *Army Training and Evaluation Program (ARTEP) 34-398-12-DRILL, Crew Drills for the AN/TLQ-17A(V)3 Trafficjam Countermeasures Set* (Washington, DC: Government Printing Office, 2004), 14-15.

[19] US House of Representatives, *Intelligence Successes and Failures in Operations Desert Shield/Storm*, Report of the Oversight and Investigation Committee on Armed Services (Washington, DC: Government Printing Office, 1993), 7-8.

[20] Alfred Price, *The History of US Electronic Warfare, Volume 3, Rolling Thunder Through Allied Force, 1964-2000*, 404, 445; Alfred Price, *War in the Fourth Dimension: US Electronic Warfare, from the Vietnam War to the Present* (Mechanicsburg, PA: Greenhill, 2001), 221.

[21] Forecast International, "ALQ-151(V) (Advanced Quick Fix)-Archived 4/2000," Airborne Electronics Forecast, April 1999, accessed January 20, 2019, https://www.forecastinternational.com /archive/disp_old_pdf.cfm?ARC_ID=32; Kevin C. Peterson, "Prophet Program Brief" (IEW&S Program Executive Office, August 2001), Kenneth T. King Personal Records; Office of the Director, Operational Test and Evaluation, "Prophet Report for the Office of the Secretary of Defense," 1999, accessed January 20, 2019, http://www.dote.osd.mil/pub/reports/fy1999/pdf/army/99prophet.pdf.

Missed Opportunities and Adaption

Far from benign, the Army's failure to evolve EW led to missed opportunities in the ripe signals environment of 2001 Afghanistan. During the drive of the Northern Alliance south through the country, the Taliban used only "Soviet-made shortwave radios," walkie-talkies, and satellite phones to communicate."[22] This environment would have been ideal for EW. Even small jammers could have overpowered the radios the Taliban was using. In November 2001, units deploying to Afghanistan were able to take newly tested Prophet systems with them to theater. The system was successful in intercepting enemy signals intelligence.[23] But the fielded Prophet was not able to jam enemy communications signals. Upgrades to include jamming were to be introduced in the Prophet Block II/III in late 2005 and 2006.[24] However, the Army never developed expected jamming upgrades. No other EW solution was fielded to conduct EW jamming of Taliban communications.

Subsequent generations of the Prophet platform increased the capabilities of the Prophet system but still did not address EW capabilities. The Prophet "Hammer" and "Spiral" versions, for instance, increased the frequencies in which the Prophet could collect. The Prophet "Triton" version in 2006 allowed a unit to effectively "identify and locate the origins of enemy" communications.[25] The last pedigree of the Prophet system, the "Prophet-Enhanced," included a

---

[22] Matthew M. Aid, *The Secret Sentry: The Untold History of the National Security Agency* (New York: Bloomsbury Press, 2009), 220.

[23] Ibid., 255-266.

[24] Maryann Lawlor, "Signal Intelligence System Uncovers Enemy Sites," *SIGNAL Magazine*, October 2002, accessed January 21, 2019, https://www.afcea.org/content/signal-intelligence-system-uncovers-enemy-sites.

[25] Aid, *The Secret Sentry: The Untold History of the National Security Agency,* 279.

myriad of features useful to signals intelligence collection. However, none of these versions had an EW jamming capacity.[26]

In 2006 the AN/VLQ-12 CREW Duke System was developed to counter the RC-IED threat. The Army fielded CREW Duke to forces in Iraq to counter the insurgency's Improvised Explosive Device (IED).[27] The CREW Duke System, one of many eventual counter-IED systems, changed the way the Army approached EW. The system was integrated into vehicles and developed a "bubble" which targeted frequencies used by insurgents to detonate Radio-Controlled Improvised Explosive Devices. The Army trained integration of CREW Duke systems into patrols and convoys.[28] The system actively searched and jammed specific frequencies so that insurgents could not detonate Radio Controlled Improvised Explosive Devices on US soldiers.[29]

The CREW Duke System redefined how the Army employed EW, changing its emphasis from an attacking to a defensive role. No longer was Army EW focused on a specific capability delivered only by a few platforms, such as the TLQ-17 Trafficjam. It was now a ubiquitous capacity wielded by a large percentage of the force. Instead of precisely targeting enemy units or denying command and control to an area before an attack, it developed a persistent capacity wherever US forces were present.[30] This was a tactical solution that partially answered the

---

[26] Michael Popovich and Jonathan B. Slater, "Prophet Enhanced NMIB" (Prophet Product Manager, March 20, 2014), Kenneth King Personal Records.

[27] J. Elise Van Pool, "CREW: Helping Defeat IEDs," *US Army*, October 26, 2011, accessed January 21, 2019, https://www.army.mil/article/67963/crew_helping_defeat_ieds.

[28] Ronald Metternich, "Counter-IED Road to War" (National Training Center, December 2, 2007). Kenneth King Personal Records.

[29] Leonardo DRS, "Short History of Army Electronic Warfare," accessed January 21, 2019, https://www.leonardodrs.com/sitrep/q1-2016-the-invisible-fight/short-history-of-us-army-electronic-warfare/.

[30] Andrew Stevens, "Ground Crew Leader's Brief" (Project Manager Signal Warfare Overview, October 22, 2005), Slides 54-59. Kenneth King Personal Records.

strategic objective of force protection from Radio Controlled Improvised Explosive Devices. The Air Force, for its part, developed many of the same ideas regarding EW much sooner.

Air Force: Integrating Technology

The Air Force was already heavily invested in EW by 1973 due to experiences with strategic and air radar jamming in World War Two. However, the Arab-Israeli War influenced decisions to modernize its fleet. Most significantly, the Air Force developed the EF-111 Raven Aircraft in 1974. The EC-130 "Compass Call," produced in 1982, is used to conduct electronic attacks but also collected SIGINT. The Air Force consistently advertised EW capability to the force. Leaders were made aware of their capabilities and tactics through exercises in the 1980s and 1990s.

The 1987 "Bright Star" exercise is an excellent example of how seriously the Air Force took EW. The exercise was conducted jointly with Egyptian armed forces. It had EW as its centerpiece, with two of its four objectives focused on the Soviet-built Egyptian integrated air defenses. The Compass Call and EF-111 Ravens, along with many other fighters, bombers, and support aircraft participated in the exercise. One note from the official after-action review was that "electronic combat training was outstanding."[31] Without knowing it, the Air Force was directly training for the 1991 Gulf War in which the United States found itself against another Soviet-developed integrated air defense system.

Both the EF-111 Raven and Compass Call saw substantial use during the Gulf War due to their effectiveness. The platforms were given important mission sets during the initial stages of the war in the suppression of air defenses. As the war progressed, smaller Air Force strike packages made direct support EW impractical. Additionally, the threat from the Iraqi integrated air defense system was limited to mobile surface-to-air missile systems, making them hard to jam.

---

[31] Eliot A. Cohen, *Gulf War Air Power Survey, Volume IV: Weapons, Tactics, and Training and Space Operations* (Washington, DC: Government Printing Office, 1993), 400.

Thus, air planners gave EW aircraft established orbits within the theater of operation to maintain a continuous quick-reaction EW support if needed. The Compass Call was used primarily as a method to surveil the Iraqi command and control network. While official histories note that the Compass Call was "effective in disrupting voice systems," histories note it was also "underutilized" because of Iraqi emphasis on communications security. When it was available, the Compass Call was effective in jamming nearly everything in range.[32]

The Air Force's focus on multi-role aircraft after the Gulf War removed the EF-111 Raven from service and outfitted many aircraft with jamming packages. The EF-111 Raven was too specialized to be useful in the future Air Force concept of warfare. The EF-111 Raven, for instance, had the significant draw-back of not being able to carry missiles, specifically High-Speed Anti-Radiation Missiles. The advent of multi-role fighters meant that the same aircraft could house AN/ALQ-99 (or upgraded) jamming technology and carry missiles, to include the High-Speed Anti-Radiation Missile-variety. This allowed aircraft, specifically the F-16C Fighting Falcon in the early 1990s, to provide organic electronic countermeasures. This organic capability decreased the need for additional direct support EW aircraft in that role.[33] Unfortunately, the fleet size of the Compass Call, the most significant EW capable aircraft that supported ground forces, has only increased marginally since the Gulf War. In 1991, the Air Force had eight Compass Calls in its fleet.[34] Since then, the number has grown to 15, with the last airframe fielded in 2001.[35] The decrease in airborne EW platforms affects the Army, which depends on EW coverage from above.

---

[32] Cohen, *Gulf War Air Power Survey, Volume IV: Weapons, Tactics, and Training and Space Operations,* 93-97.

[33] Martin Streetly, *Jane's Radar and Electronic Warfare Systems: 2011-2012* (Alexandria, VA: Jane's Information Group, 2011), 585-626.

[34] Bernard Blake, *Jane's Radar and Electronic Warfare Systems: 1991-1992* (Coulsdon, Surrey; England: Jane's Information Group, 1991), 433.

[35] Streetly, *Jane's Radar and Electronic Warfare Systems: 2011-2012*, 795.

Air Force Comparative Advantage leads to Army Electronic Warfare Divestiture

Dedicated EW capability across the defense services decreased since the Gulf War as the Air Force divested EW-specific platforms for multi-role aircraft, a decision based on advances in technology and the capability to have dedicated radar jamming in each of its air platforms. The discussion above, regarding the capabilities and the issues with specific systems associated with the Army, Air Force, and Navy, is essential for several reasons. The first is that any platform with EW capability does not just have tactical implications. The scarcity of these systems dictates that their employment effects how US forces move throughout a theater. Secondly, the Army has determined historically that ground-based EW has limited effectiveness and that it is easier to request that capability from a more effective air component. During the Gulf War, this was significantly the Compass Call to suppress enemy command and control nets.[36] However, the problem is that the Air Force itself has decided to divest aircraft that only conduct EW and has determined to focus on defensive EW as a part of multi-role aircraft designs. Just as the Air Force did with multi-role fighters, the Army has curtailed EW capability platforms in preference to incorporating electronic counter-measures into existing combat platforms.

Marine Electronic Warfare: by Way of Air and Ground

Unlike the Army, the Marine Corps, as a ground and air (and sea) component, was able to develop and maintain EW capacity. The EA-6B Prowler, one of the best and oldest EW air platforms in the US Military, was developed for the Marine Corps in the 1960s. Until 2019, the Marines maintained the EA-6B Prowler as their primary airborne EW capability. The aircraft has been in service since 1971 and the Marines still use it in combat. The Air Force also relied on the

---

[36] Cohen, *Gulf War Air Power Survey, Volume IV: Weapons, Tactics, and Training and Space Operations*, 96-97.

Navy's EA-6B Prowler for EA operations during the 1991 Gulf War.[37] The Corps now uses the

F-35B "Lighting II" as its aerial EW capability.[38]

With regard to ground-based EW, the Marine Corps has paralleled Army capabilities.

The Marines developed the CREW Vehicle Receiver Jammer alongside the Army's CREW Duke

System, with similar capabilities. Additionally, the Corps continues to work with the Army to

develop better ground-based solutions as the technology advances.[39]

Conclusion: Implications of Electronic Warfare Improvidence

The implication in the trends of EW capability is that the Army, and its EW proponent

the Intelligence Branch, did not appropriately anticipate changes in EW technology. The

Intelligence Branch did not correctly forecast the movement from a specified EA capability in

one or a couple of platforms to the diffuse capacity of the CREW Duke systems. The Intelligence

Branch focused on problem-sets within its purview. The diffusion of EW capability is a broader

Army initiative that requires inter-branch, and in some cases, joint emphasis. However, the

pendulum seems to be swinging back as the Army again grapples with how to develop an EA

component of its ground forces.

The Army is again attempting to infuse EW capability into corps, division, and brigade

echelons but this may be counterproductive to long-term EW efficacy. The role EW will play on

any future battlefield may have evolved at the tactical level with the perfusion of jamming

---

[37] Cohen, *Gulf War Air Power Survey, Volume IV: Weapons, Tactics, and Training and Space Operations*, 93-95.

[38] Dustin Mullin, "Navy Growlers Train with Air Force, Marines during Red Flag 17-3," Nellis Air Force Base, July 26, 2017, accessed February 7, 2019, https://www.nellis.af.mil/News/Article/1262522/navy-growlers-train-with-air-force-marines-during-red-flag-17-3/; Shawn Snow, "The Corps Is down to One Final EA-6B Prowler Squadron," *Marine Corps Times*, May 30, 2018, accessed February 7, 2019, https://www.marinecorpstimes.com/news/your-marine-corps/2018/05/16/the-corps-is-down-to-one-final-ea-6b-prowler-squadron/.

[39] Mark Pomerleau, "For Better Electronic Warfare, the Army and Marine Corps Work Together," *C4ISRNET*, July 19, 2018, accessed January 21, 2019, https://www.c4isrnet.com/electronic-warfare/2018/07/19/for-better-electronic-warfare-the-army-and-marine-corps-work-together/.

capability due to smaller and better technologies. The Intelligence Branch, with its focus on SIGINT, has proven to be parochial of core competencies at the expense of emerging capability in EW.

The future will determine the efficacy of such an argument, but the historical trends support the assertion that, tactically, a synchronized electronic attack is less significant than electronic counter-measures. The Intelligence Branch's policies emphasizing intelligence gained from communications networks as more critical than jamming is well-intentioned but conventional operations do not usually lend themselves to that level of fidelity. At the point that Army forces engage conventional enemy forces, and the same could probably be applied to Air Forces as well, jamming is historically the better option. Thus the use of diffuse EW systems associated with combat platforms, as was piloted by the CREW Duke System and the Air Force's emphasis on multi-role fighters, may be a superior method of employment.

The larger Army has not helped the Intelligence Branch in developing EW, nor recognized that the discipline has outgrown the proponency of one branch. The Army has placed EW proponency in limbo since 2005, partially vindicating this viewpoint. In 2005, the Fires Branch became the proponent of EW and then, in 2018, it was transitioned to Cyber Command. This juggling implies that EW may not belong to any specific branch and instead is a capability to be used across units and combat platforms. EW may be used best when not limited to a few select EW units, platforms, squads, or to one specific branch.

Electronic Warfare Organizations and Doctrine

Since the 1970s when modern EW ideas took root, the electromagnetic spectrum has gotten more crowded, the Army warfighting concepts have evolved, and the force structure of EW organizations has shifted. Despite all of this change, ideas related to EW employment did not dramatically transform in the Army until the 2001 Global War on Terrorism. Even then, jamming technology was in response to Radio Controlled Improvised Explosive Device threats. Despite

macro changes in battlefield framework, some micro subcomponents, such as EW, remained relatively static. New doctrine in the 1970s led to the acceptance of EW as a significant capability, but subsequent Army-wide doctrinal changes decreased the emphasis placed on the discipline. Units, which included EW, also reached their zenith in the 1980s, only to be dissolved later due to changes in the Army's concept of warfighting. In this respect, the Intelligence Branch was both a part of a larger Army trend and a contributing factor towards de-valuing EW by not emphasizing the discipline in its doctrine and organizational structures. Army concepts of EW employment have been primarily reactionary because of doctrinal and organizational parochialism. The formation and eventual atrophy of EW capability within the Army was predicated by larger conceptual movements unrelated to the EW discipline.

Training and Doctrine Command Champions Electronic Warfare

Without the development of Training and Doctrine Command (TRADOC) in 1973, EW would not have found traction within the Army. The new TRADOC organization tapped into lessons learned derived from the 1973 Arab-Israeli War, to remake the post-Vietnam conventional Army. General William DePuy, having served in World War Two and Vietnam, became the commander of the TRADOC. His mandate from the Army Chief of Staff, General Creighton Abrams, was to remake the Army. The Army, still reeling from its experience in the Vietnam War, needed a new paradigm. General DePuy did not have to look long. DePuy took the reins at TRADOC in July 1973, and by October, a coalition of Arab states attacked Israel in a modern and staccato conventional war.[40]

DePuy's emphasis on EW likely evolved from his belief in American firepower as a combat multiplier. DePuy took the lessons of World War Two forward with him to Vietnam. He emphasized firepower as a means to defeat enemy forces while protecting American lives. This

---

[40] John L. Romjue, *From Active Defense to AirLand Battle: The Development of Army Doctrine 1973-1982* (Fort Monroe, VA: United States Training and Doctrine Command, 1984), 3-4.

mindset influenced DePuy to search for technological solutions in the hopes that he could

realistically match growing Soviet military power in Europe. This concept, vindicated through his

experience in Vietnam, favored artillery preparation. [41] EW was no doubt a component of that

same outlook; also perhaps foreshadowing EW jamming's conceptual relation to the Fires

Branch. The idea that the electromagnetic spectrum may achieve operational objectives while

saving Soldier's blood very likely was a consideration. TRADOC's read of the 1973 Arab-Israeli

War supported these proclivities.[42]

The combination of Active Defense and technological constraints focused EW within the

context of a defensive war in the European Theater against the Union of Soviet Socialist

Republics (USSR). The influence of the real and present threat of the USSR meant that the Army

would most likely be fighting a defensive war. The very name Active Defense is an apt

description of the doctrine's primary theme. To their credit, DePuy and TRADOC did

meticulously include chapters on the offensive, but critics paid more attention to the overarching

concept. The emphasis on the defensive was one of the major criticisms of Active Defense

doctrine. [43] It was also the concept which EW was focused and the environment in which EW

technology matured. Thus the Trafficjam, the Army's EA platform, fielded to CEWI battalions

and brigades was created in the mid-1970s under the auspice of Active Defense doctrine. Due to

wide-spread disapproval of Active Defense, a replacement warfighting concept called "AirLand

Battle" quickly came to the forefront. However before that transition, Active Defense put in

motion a series of reforms related to EW which had a significant impact on the future of the

discipline.

---

[41] James Scott Wheeler, *The Big Red One: America's Legendary 1st Infantry Division from World War I to Desert Storm* (Lawrence, KS: University Press of Kansas, 2007), 398; Romjue, 5.

[42] Romjue, *From Active Defense to AirLand Battle: The Development of Army Doctrine 1973-1982,* 5.

[43] Ibid, 14.

Exploiting Electronic Warfare

For the Intelligence Branch, EW was a means to an end and not necessarily a justification in and of itself for organizational and doctrinal changes within the branch. As the Army's concept of warfare changed throughout the 1970s and 1980s, the idea of EW as a useful function within divisions and corps decreased. By the 2000s, at the onset of Army modularity initiatives, EW was not something that was seriously pursued and withered as a capability. Two contributing factors led to the incorporation of EW by divisions and corps. The first was the Army's development of Active Defense doctrine in the mid-1970s. The second of those were lessons learned about the integration of all types of intelligence during the Vietnam War.

The nexus of Army incorporation of EW was Combat Electronic Warfare Intelligence (CEWI) units, which integrated EW and various intelligence disciplines in one organization. The Intelligence Branch fielded CEWI battalions (figure 2) and brigades beginning in 1979 through the 1990s, significantly transitioning the organizational make-up of the Army Military Intelligence (MI) community.[44] The roots of the CEWI battalions and brigades reside in lessons learned from the Vietnam War. Primarily, CEWI units developed due to a consistent movement of Army intelligence leadership to consolidate signals intelligence (and its sub-discipline at the time, EW) into other intelligence capabilities that included human, imagery, and radar intelligence.[45]

---

[44] Daniel Baker, "Deep Attack: A Military Intelligence Task Force in Desert Storm," *Military Intelligence Professional Bulletin* 34-91–4 (December 1991): 39-42.

[45] Finnegan and Danysh, *Military Intelligence,* 180-81.
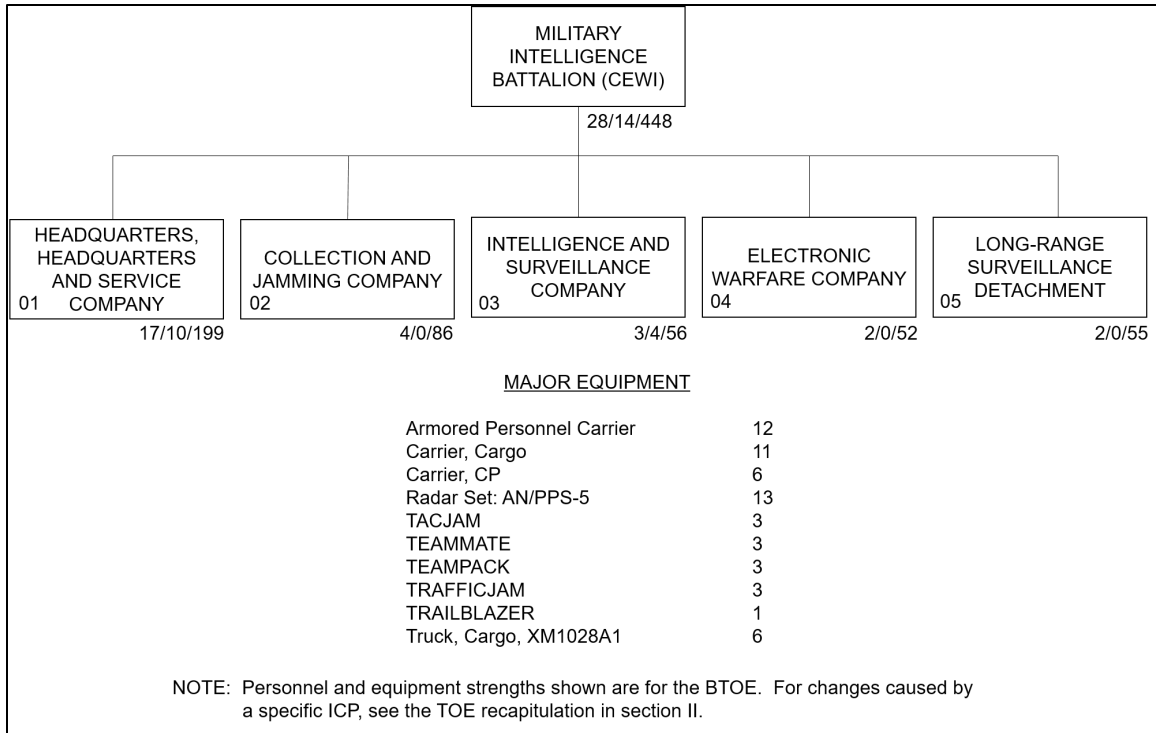
Figure 2.   Military Intelligence Combat Electronic Warfare and Intelligence Organization Diagram
Source: US Department of the Army, *TOE 34285L-CTH*, *Commander's TOE Handbook: Military Intelligence Battalion, Division* (Washington, DC: Government Printing Office, 1990).

As a part of the initiative to reform intelligence units based on these ongoing lessons from the Vietnam War, the Intelligence Branch commissioned the Tactical Reconnaissance and Surveillance-75) Study in 1967. The study conducted several tests and exercises, one of the most significant being in October 1969, which validated a structure to bring a SIGINT company of the ASA under the direct control of the exercise's division commander.[46] By 1969, ground-based EW was only beginning to be a viable technology and so was not included in the study, but EW equipment was developed by the Army in the succeeding years.[47] The Military Intelligence

---

[46] Sidney T. Weinstein, "Evolution of Military Intelligence" (Memorandum for Military Intelligence Personnel, Fort Huachuca, AZ, January 3, 1984), 4. Kenneth King Personal Records.

[47] John Pike, "AN/TLQ-17A(V), TRAFFICJAM."

Company and Battalion tables of organization and equipment generated from the study was the direct predecessor of CEWI units commissioned six years later.[48]

The CEWI battalions, developed for divisions and corps, were a massive boon for the Intelligence Branch though not necessarily, despite the name, for EW. The Army infused MI soldiers and officer leadership into the organization. The number of military intelligence officers and soldiers increased exponentially during this period.[49] It was the nadir of intelligence units within the Army. CEWI units included six communications jamming teams, within a Collection and Jamming Company.[50] This Collection and Jamming Company added a wide array of intelligence platforms, to include signals intelligence. The EW capability, located alongside a platoon of signals collection soldiers, formed the company. What used to be an attachment of soldiers from the ASA, was now integrated under the direct command of division and corps commanders. Integration of ASA soldiers with the rest of the Army's Intelligence Branch was part of a more substantial Army effort to remake itself under the newly christened TRADOC.

Electronic Warfare Concepts Begin to Change

In 1978, DePuy's successor at TRADOC, General Donn A. Starry began the first of what would become several studies under the heading "Division 86." These studies experimented with organizational changes associated with the emerging concept of AirLand Battle. The 1982 version of Field Manual 100-5 *Operations,* the first to extoll AirLand Battle concepts, maintained the efficacy of EW, but relegated the capability to defense and deception. Specifically, the manual notes that commanders should use jamming assets to simulate artillery radars as a part of

---

[48] Weinstein, "Evolution of Military Intelligence," 9.

[49] US Department of the Army, *TOE 34285L-CTH*, *Commander's TOE Handbook: Military Intelligence Battalion, Division* (Washington, DC: Government Printing Office, 1990).

[50] Ibid.

deception operations.[51] EW capacity to conduct jamming of "enemy agents, saboteurs, Spetznaz teams, and airborne/airmobile units" was also prescribed.[52] AirLand Battle doctrine noted that EW would "be directed against the forward and rear areas."[53] However, the contradiction was that ground-based EW capabilities of the Army could not independently do so, thus AirLand Battle, without directly stating so, emphasized Air Force EW as a capability. Whatever the divisions and corps were unable to influence would be requested from echelons above corps organizations. For example, the 1982 Field Manual 100-3, *Operations* notes that Army EW units at echelons above corps will interface with Air Force, Navy, and other national agencies to fill gaps in Army EW capabilities.[54] The method of EW as a deception tool was only one of many ways that doctrine suggested artillery officers use EW to their advantage.

Within the AirLand Battle concept, EW is mentioned explicitly within the context of its use in conjunction with artillery, rather than intelligence. Additionally, AirLand Battle doctrine notes that the co-located Fires and EW Element at the division echelon is the most effective.[55] The imagined link between fires capability and EW no doubt shaped how the Intelligence Branch considered the EW discipline.

After its ascendance in 1975, the CEWI construct of integrated EW and intelligence precipitously declined. The attrition of intelligence billets within divisions and corps, and the Army as a whole, contributed to the deterioration of EW capability. Due to budget cuts, personnel challenges, and modularization, the Army allocated fewer and fewer billets to the Intelligence

---

[51] US Department of the Army, *Field Manual (FM) 100-5, Operations* (Washington, DC: Government Printing Office, 1982), 7-19.

[52] Weinstein, "Evolution of Military Intelligence," 4-9.

[53] US Army, *(FM) 100-5* (1982), 1-2.

[54] Ibid., 6-4.

[55] Ibid., 7-19.

Branch.[56] As an unproven capability within the construct of AirLand Battle, the Army cut EW billets from the division and corps echelons.[57] As previously mentioned, research and development on updated equipment were also curtailed or re-programmed for future budgets.[58] The Army fielded the last CEWI battalions in the 1990s. Shortly thereafter, beginning in 2004, the Army's modularity initiatives separated CEWI units from divisions and corps; by this time tables of organization and equipment referred to them as Military Intelligence Battalions and Groups, respectively. Signals intelligence teams were still managed by brigades, but EW capability was not. EW teams were only allocated at division and below through Training and Readiness budgets or a Joint Strategic Capabilities Plan during a deployment.[59]

By the advent of the Army's Full Spectrum Operations concept of warfare in 2008, there is even less mention of EW as a critical element. The 2001 version of Field Manual 3-0 groups EW under Information Operations, along with deception, security, and cyber.[60] EW proponency primarily transitioned to the Fires Branch in 2005. The Intelligence Branch maintained the "electronic warfare support" function, mainly the responsibility to support EW with signals intelligence.

Electronic Warfare saw a small renaissance during Operations Iraqi Freedom and Enduring Freedom due to counter radio-controlled IEDs. But, the capability was used for a very narrow range of combat effects. After the transition to the Fires Branch, the Army's operational

---

[56] US Army, *TOE 34285L-CTH* (1990).

[57] Ibid.

[58] Government Accounting Office, *Electronic Warfare: Test Results Do Not Support Buying More Common Sensor Systems* (Washington, DC: Government Printing Office, 1998), 3.

[59] US Army Intelligence Center of Excellence, "U.S. Army Computer Network Operations-Electronic Warfare Proponent (USACEWP)" (Slide Presentation, CW2 Christopher G. Nason Military Intelligence Library, Fort Huachuca, AZ, 2008).

[60] US Department of the Army, *Field Manual (FM) 3-0, Operations* (Washington, DC: Government Printing Office, 2001), 11-19 – 11-20.

EW capability unequivocally declined, even under new management it was not expected to be needed by all corps and divisions. Additionally, there was no further progression of EW platforms. This status quo has continued, even with slight interest by the Army during counterinsurgency operations in Iraq and Afghanistan.

Contemporary Electronic Warfare

The movement to large-scale combat operations and the belief that US competitors, primarily Russia, developed significant EW capability beyond Army technology has spurred a revolution in EW development. As the Obama Administration ended major combat operations within Iraq in 2011, the Army took a turn to its World War Two history and aimed to return to large-scale combat operations as the *raison d'être* for the conventional Army. Along with this belief was the additional understanding that while the Army innovated for Iraq and Afghanistan, its adversaries developed the next generation of conventional weaponry. Russian incursions in Ukraine in 2014 confirmed this view. Russian weapon demonstrations within the Syrian Civil War expanded this belief. Among demonstrations of Russian technology were EW capabilities that surpassed US capability.[61] To address this gap, the United States began to field EW soldiers and technology to the Army in 2010, but the effort is still in its infant stages.[62] However, this renewed emphasis on EW to catch-up with Russia tactics has little unity of direction.

To address observations of Russian EW advancement, the Army has begun to field EW systems and address gaps in concepts. The main systems, fielded as test units are the "Sabre Fury," which is a vehicle-mounted jammer and the "Versatile Radio Observation and Direction

---

[61] Liam Collins, "Russia Gives Lessons in Electronic Warfare," *Association of the United States Army*, July 26, 2018, accessed January 24, 2019, https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare.

[62] Mark Pomerleau, "New Electronic Warfare Program Tops Army Intel Wishlist," *C4ISRNET*, March 6, 2018, accessed January 24, 2019, https://www.c4isrnet.com/electronic-warfare/2018/03/06/new-electronic-warfare-program-tops-army-intel-wishlist/.

Modular Adaptive Transmit" (also referred to as VMAX). However, the improved jamming equipment, which is still not integrated into an overall warfighting concept. Nor is the EW mission appropriately resourced with personnel or vehicles.[63] Observations from Russian operations in the Donbas, Ukraine, and Crimea have still not been addressed and is a capability gap which can be exploited.

Conclusion: Implications of Electronic Warfare Temporization

The EW discipline will have to undo decades of neglect to maintain relevancy compared to foreign EW capability. The Intelligence Branch, swept along and eventually aside in the devaluation of EW, did not provide diligent proponency of EW. Instead of searching for where EW could be most useful, the branch used concepts and fascinations with EW to further its own goals of integration with the ASA Signals Intelligence Branch. Additionally, the Intelligence Branch never fully developed EW doctrine, and thus the larger Army continued to decrease the role of EW in conventional combat operations. It is only due to recent conflicts in which foreign nations showcased EW that the nation has modestly begun to rebuild EW capacity as a starting point.

The Army Security Agency: An Almost Proponent of Electronic Warfare

While larger trends in doctrine and Army organization affected the growth of EW, the Intelligence Branch's internal bureaucracy played an even larger role. The ASA, previously the Army's Signals Intelligence Branch before all intelligence disciplines were amalgamated in the 1970s, was the organization directly responsible for EW after acquiring the discipline from the Signal Branch in 1955. However, the ASA's core competency was SIGINT; it was one of the

---

[63] Robert F. Behler, *Director, Operational Test and Evaluation FY 2018 Annual Report* (Washington, DC: Government Printing Office, 2018), 79-80; Mark Pomerleau, "How Will the Army Use Electronic Warfare? The Pentagon's Weapon Tester Wants to Know," *C4ISRNET*, February 5, 2019, accessed February 7, 2019, https://www.c4isrnet.com/electronic-warfare/2019/02/04/how-will-the-army-use-electronic-warfare-the-pentagons-weapon-tester-wants-to-know/.

main contributors to the nation's intelligence community during that time. The relationship from 1955 through the early 1970s was rocky, but not overly so because the technology for ground-based EW was not yet viable. It was not until after the 1973 Arab-Israeli War that the confluence of technology and interest existed for Army leadership to begin asking questions about EW. One of the questions Army and civilian leadership were asking was, "why." Why was the ASA not developing EW capabilities?

Brigadier General George Godding, the commander of the ASA from March 1973 to August 1975, was metaphorically bailing water out of a sinking boat during his tenure.[64] The Army wanted to shutter the ASA, which was in charge of EW for the Intelligence Branch, to make the entire branch more efficient.[65] Godding did not believe this was in the best interest of the nation. He embarked on a crusade to educate Army commanders to use EW and SIGINT in their organizations effectively.

The ASA did not prioritize EW from 1955 to 1976, during which period that the agency was the proponent of the discipline, but once the ASA reflagged and EW was de-centralized, there was no direct leadership guiding the EW discipline. After that time, no organization directly drove EW adaptations to changing Army missions and technology. Due to the Army's transitioning concept of war towards Active Defense, and later AirLand Battle, there was a shift in the mission of the ASA during those years.

Problems with the Army Security Agency

The ASA had several attributes which were not compatible with emerging doctrine. The first was its focused on strategic rather than tactical objectives. The ASA had become a very

---

[64] US Army Intelligence Center of Excellence, "Major General George A. Godding Military Intelligence Hall of Fame Biography," accessed January 21, 2019, https://www.ikn.army.mil/apps/ MIHOF/biographies/Godding,%20George.pdf.

[65] Finnegan and Danysh, *Military Intelligence,* 179-180.

efficient organization, providing useable strategic intelligence to America's decision makers, keeping tabs on enemy militaries. Limited resources and its strategic focus undermined the ASA's utility to corps and division commanders.[66] Second, as a corollary to its strategic mission, the ASA was focused mostly on communications intelligence, listening to what people were saying on communications platforms, rather than electronic intelligence, where communications emissions were coming from and what they were.[67] While the military can use both communications intelligence and electronic intelligence against national targets as well as tactical military targets, electronic intelligence is useful to EW jamming because it is targetable. Third, the ASA was a stove-piped organization that was parochial. The organization's autonomy had slowly been whittled away through a series of reforms in the 1950s, to include the development of the Pentomic Division, and lessons learned from the Vietnam War.[68] However even though the ASA had lost ground, it still played a large role in tactical efforts.

The ASA still administratively and technically controlled SIGINT and EW units even if they were attached to divisions and corps.[69] The reason for this control, more than bureaucratic turf wars, was that it was necessry due to limitations of equipment and intelligence processing. The entire weight of the ASA, funneled through the SIGINT and EW team co-located with the unit, was much more effective in answering collection requirements in a holistic and timely

---

[66] George A. Godding, "An InnerView of ASA as Seen by General Godding," *The Hallmark: United States Army Security Agency* 8, no. 8 (September-October 1975): 14-16.

[67] Aid, *The Secret Sentry: The Untold History of the National Security Agency*, 163-65; Duncan Brown, "Last Gasp of the ASA," ASA Lives, accessed January 22, 2019, http://www.asalives.org/ASAONLINE/lastgasp.htm.

[68] Finnegan and Danysh, *Military Intelligence,* 142-43.

[69] Godding, "An InnerView of ASA as Seen by General Godding," 14-16.

manner than the dedicated 12-person squad with limited radio intercept equipment. An additional consideration was the secrecy required to maintain overmatch in SIGINT and EW.[70]

Lastly, and most important element as it relates to EW, the ASA was a collection agency and so EW functions were not emphasized as part of its mission through most of its history. The inherent secrecy of the ASA "excluded the rest of the Army from involvement in the vital electronic warfare field."[71] The ASA reported to the Director of the National Security Agency, the national signals intelligence agency. As such, the ASA's EW capability languished. The ASA's mission had four aspects of which only strategic signals intelligence was pursued at the expense of its role in signal security, direct support to tactical SIGINT, and electronic warfare. The lack of emphasis on EW was not only evident operationally, but prevented ASA "from keeping up with new trends in electronic warfare."[72]

The reason the ASA did not emphasize EW was because of many of the organization's structural problems and understanding of how they were supposed to support the Army. Since there was a low-level of ASA presence at the corps and division echelons, coupled with the secrecy of the organization, commanders had a minimal understanding of how to use ASA attachments effectively. There was almost always a degree of separation between fielded ASA units and the commanders through which they reported. Mostly, reporting was conducted through the unit's Special Security Office and the G2 intelligence staff section. While this relationship caused issues with intelligence timeliness and anticipation of requirements, ultimately there was little friction. Collection of signals intelligence, after all, is mostly a passive endeavor and in the event a commander has to act without proper intelligence he can elect to do so. Such a

---

[70] For examples of ASA information through teams co-located with units see: Douglas W. Bonnot, *The Sentinel and the Shooter* (Livermore, CA: WingSpan Press, 2010).

[71] Finnegan and Danysh, *Military Intelligence,* 302.

[72] Ibid.

relationship does not exist for EW. Electronic Warfare, like artillery, has to be actively used and integrated into the commander's plan.[73]

Army Security Agency to Intelligence and Security Command Transition

With all this in mind, General Godding believed he could reform the ASA. He believed that a re-orientation to tactical usefulness, especially at the division echelon, was key to the reform. But General Godding was fighting against the bureaucratic forces as the friction point between the military's thirst for strategic intelligence versus the Army's tactical intelligence in a future conflict. Despite the Intelligence Organization Stationing Study recommendation to re-focus on a tactical mission, the ASA was not structured or funded to support those recommendations. In 1976, the ASA was receiving 90 percent of its funding to support strategic intelligence gathering, the remainder on tactical intelligence and EW.[74] Such a transition would take time that General Godding did not believe he had. Limited in his ability to re-allocate funding and re-structure the ASA in a short time-period, he thought education of leaders of what ASA did might forestall these drastic changes.[75]

A campaign to educate senior leaders on the roles of the ASA, how the ASA could accomplish its tasks, and how commanders could better utilize their ASA elements was rolled out. Godding stressed that it was the EW elements which were getting under-worked. He emphasized the need for EW to work in conjunction with the unit's fires cell to be employed offensively within the unit's scheme of maneuver.[76]

---

[73] Godding, "An InnerView of ASA as Seen by General Godding," 14-16.

[74] Brown, "Last Gasp of the ASA."

[75] Godding, "An InnerView of ASA as Seen by General Godding," 14-16.

[76] Ibid.

On September 1, 1975, Brigadier General William I. Roya replaced General Godding. Roya had been Godding's deputy commander since May of the previous year. Roya transitioned the ASA into a larger, newly created Army military intelligence organization named the Intelligence and Security Command (INSCOM). He completed ASA's transition and took command of INSCOM in January 1977. The new organization brought all the diverse strategic intelligence organizations, such as the Assistant Chief of Staff for Intelligence and US Army Forces Command intelligence production elements, under its control. In the same stroke, ASA elements previously only attached to corps and division echelons now reverted to organic units, eventually to be part of the Army's emerging CEWI units.[77]

The development of INSCOM drastically changed how the Army treated intelligence and EW. Some changes aligned EW assets with the units that could use them, while INSCOM gained direct control of other assets. Above the corps echelon, "INSCOM provided the Army with a single instrument to conduct multidiscipline intelligence and security operations and electronic warfare."[78] Under INSCOM, many of the EW programs continued that had been started by the ASA. However, in the ASA, EW lost proponency by an organization that included a focus on corps and division EW efficacy. Roles and responsibilities across the Army intelligence discipline operated in a state of flux into the 1980s as INSCOM, TRADOC, and US Army Forces Command expediently addressed shortfalls in intelligence and, to a lesser extent, EW.

Conclusion: Forfeiture of an Army Security Agency Alternative

Much like General Godding, leadership in INSCOM was not able to advance the EW discipline before being overcome by events. By the 1980s CEWI units had spread; intelligence and EW capability were at an all-time high. Post-ASA, there was even less oversight of EW and

---

[77] Finnegan and Danysh, *Military Intelligence,* 174-179.

[78] Ibid., 175.

future planning for the discipline. EW had ridden the coattails of the military intelligence build-up to its benefit but also its detriment. As the Cold War came to a close in 1989 resources starting to decrease and the military intelligence field, already peaked regarding personnel, was on the decline. EW capabilities and its mission declined in tandem.

The ASA, despite its neglect of EW, was a helpful guiding hand to modernize EW. Decentralized EW, as a unique element of the Army Military Intelligence Branch, received less attention than other intelligence functions. While the ASA did not devote significant organizational energy to the discipline, they still maintained a similar capability in SIGINT collection. The ASA had leaders who knew it was their mission to advance EW and could affect change.

Conclusions and Recommendations

The Army is making the same mistakes with EW going forward as it made with the capability while part of the Military Intelligence Branch. Allowing proponency of EW by the Fires Branch and now Cyber Command guarantees that EW will not be a priority capability set, or that it will be narrowly defined to support the proponent suite of other capabilities. While there may not need to be an EW Branch, leadership with the ability to make acquisitions and influence the methodology of how the Army employs EW is necessary.

The Army Military Intelligence Branch failed to be an effective proponent of EW, leading to its decline as a capability to the present day. Several indictments can be leveled against the branch. Above all, the Intelligence Branch failed to imaginatively develop EW into something compelling for the Army's operational doctrine. The Army still struggles with this today. However, a broader perspective about developments by other services, enemy EW capabilities, and sustained organizational focus could have developed EW into a combat multiplier. The signs were and still are available to help better develop EW for the future.

First, ground-based EW is comparatively less effective than air-based platforms primarily used by the Air Force. However, this does not mean that EW could not have been developed to target niches on the electromagnetic spectrum that would have been useful. Instead, Army leadership ceded EW capability to the Air Force because of its focus on the discipline due to its use in combating integrated air defense systems. Increased height and speed make air-platforms, *caeteris paribus*, better EW systems. However, Russian operations in the Ukrainian Donbas illustrate that specialized sustained ground-based EW can be useful in isolating a battlefield.[79] Additionally, the proliferation of air-based EW would eventually provide the model for the CREW Duke counter-IED system, a model that can perhaps be expanded to conventional operations as well.

Also, the position of EW within the MI Branch, specifically within ASA, as well as the eventual re-flagging of that organization's mission decreased the effectiveness of the Army's EW capability. The ASA had its faults which negatively impacted the development of EW. Primary among these was the secrecy which the agency operated under and the vertical stove-pipe which existed within the organization. Secrecy, coupled with the prioritization of signals intelligence by the organization, meant that the Intelligence Branch did not provide the opportunities EW could otherwise have had. Additional problems were related to EW's "offensive" capability within an organization which was chartered to conduct "passive" intelligence operations. Despite the awkward relationship, the demise of ASA in the mid-1970s also limited leadership focus on EW's future development. Lack of a leader's vision eventually led to its de-emphasis except within the counter-IED fight.

Electronic Warfare can be integrative and also specialized. As was demonstrated during counter-IED efforts in Iraq and Afghanistan, EW should span combat platforms and be de-

---

[79] Michael Kofman et al., *Lessons from Russia's Operations in Crimea and Eastern Ukraine* (Santa Monica, CA: RAND Corporation, 2017), 10, 17, 25, accessed January 22, 2019, https://www.rand.org/pubs/research_reports/RR1498.html.

centralized so that coverage across the battlefield expands. Such a reconfiguration solves issues the TLQ-17 had of being targeted and not being in the right place to affect enemy communications. The precedent for this is the Air Force which fits a large portion of its aircraft with its own EW suites. But specialized EW platforms to target specific civilian infrastructure may be useful in the future, as it was for the Russian Military in Ukraine. In this way, proponency of EW must transcend a specific Army branch and be deeply committed to developing technologies and organizations to mitigate future threats while leverage opportunities. More than anything, the proponent of EW needs to continue to progress the capability, something the MI Branch failed to do. Moreover, this is a cautionary tale for the Intelligence Branch. It must ensure it does not emphasize core competencies at the expense of other important capabilities for which it is the proponent.

Recommendations

This monograph is admittedly scoped temporally and with regard to EW primarily within the Army. Understanding other states' development of EW, beyond passing references to Russia's Ukrainian adventure, would be significant to understanding the comparative strengths and weaknesses of US ground-based EW. It is only in understanding comparative advantages over other states that the United States can hope to operate in a multi-domain battle successfully. Additionally, there is no mention of Navy EW within this monograph to maintain focus on capabilities that significantly affected the ground war in a future conflict.

The wide range of possible future uses for EW must continually be explored. The Army cannot afford to cede the battle for the electromagnetic spectrum; it is too dependent on it and most known possible adversaries are as well. The Army must learn from the experience of the MI Branch and its proponency of EW because the de-emphasis of EW in the past is bad enough, but to continue to do so may be criminal.

A future researcher should conduct a broad survey of military-use of EW with its implications related to how the US Army could best develop the discipline. This survey needs to span the other services and other leading countries as well. Such a survey could provide the best practices and allow the Army to apply concepts that it otherwise has not imagined. One of the most significant problems with modern EW development, and how the Intelligence Branch treated the discipline, was based on sunk costs, leaning heavily on concepts and technology that the Branch had previously developed. Leadership never returned to the initial hypothesis to determine if it was still valuable. The military optimized the Trafficjam and the Quickfix for the Cold War and transitioned to the CREW Duke and CREW Vehicle Receiver Jammer systems for the Global War on Terrorism. The EW solution for the future may be somewhere in-between these two capabilities, or it may be something else entirely. But examining the solutions and being able to evaluate future possibilities flexibly will be key to EW going forward.

A future researcher needs to conduct a running analysis on the role that Cyber Command is playing in the advancement of the EW discipline. Cyber warfare is receiving a lot of attention from the defense community. Historically, EW has not thrived under an organization that had different core organizational competencies. Even if Cyber Command is labeling EW as equal to Cyber Warfare, continual monitoring of initiatives will provide the facts behind the narrative. Based on the research of this monograph it is difficult to believe that in the long-term the nation will regain superiority of the electromagnetic spectrum while the EW discipline is beholden to a cyber discipline. A continuous evaluation could ensure that the Army does not continue down this path for the next decade or longer only to realize deficiency in EW during the next war.

A future researcher should develop an inquiry into which branch, or other type of organization, needs to be the proponent for EW. Perhaps it found its home in Cyber Command but, empirically, this is unlikely. Research into redefining the parent organization and the role of that organization in the advancement of EW is the only way the nation will find itself, thirty years down the road, to have a useful EW capability. The methodology of the Signals Branch seems to

be an analogy for how EW should organize itself. Though the G6 (Signals) section of the division does not own all of the radios the unit uses, it tracks and is responsible for them. The radios are consistently employed at the soldier-level because they are useful to coordinate attacks and report to higher or lower echelons. The same level of administrative control and guidance may be useful for EW. Perhaps the transition of EW out of the Signals Branch in 1955 should not have happened. However, for such a concept to be useful, a new approach to EW must be taken. It must be an approach to fighting the discipline that is possible given current technology.

Technologically, the dispersion of EW on the battlefield now may be viable and the best method to employ the capability in large-scale conventional operations. This monograph was not meant to contend itself with the future of EW but through research it became apparent that the current trends in EW, returning to platform-specific capabilities in the same vein as Trafficjam, Prophet, or Sabre Fury may need to be altered in favor of a new paradigm within the discipline. A future researcher should investigate the viability of this paradigm shift. Is the capability to employ EW at high power against a specific target more practicable than having a perfuse capability on the battlefield with lower power output? The problem with platform-specific measures is that it is hard to determine where they need to be on the battlefield to have the most significant benefit. However, placing EW capability on every M1 Tank, Bradley Fighting Vehicle, and Stryker with the capacity to reach out to or just past the platforms engagement range could provide disruption of enemy communications when it is most significant, right before or during a tactical attack. Such an EW posture disallows coordinated attack, defense, and counterattack. There are a lot of technological hurdles associated with this recommendation which are beyond the scope of this monograph. However, lower powered omnipresent EW seems to be the trend based on research for this monograph.

Epilogue

In closing, the title "Electronic Warfare, the Intelligence Branch, and Organizational Encopresis" is a direct metaphor for the thesis of this monograph. Encopresis is a psychological

disorder characterized by "repeated passage of feces into inappropriate places (e.g., clothing or floor) whether involuntary or intentional."[80] In this metaphor, the Intelligence Branch is the organization affected by a form of encopresis. During the time of its proponency, it sometimes willfully, and sometimes inadvertently, subverted the progress of the Army's EW capability. In one case by labeling its battalions CEWI, while filling them with minimal EW capabilities. A willful subversion. In other cases, procurement of EW technology was slower than the Army's doctrinal concepts of how to fight wars. This caused EW to be outdated, an effect the Intelligence Branch did not intend. The treatment for encopresis is behavioral modification. The act of defecation may be a symptom of larger psychological issues. Metaphorically the same idea is pertinent to organizations. The Intelligence Branch should take this to heart and re-evaluate its relationship with EW. A similar process is required to renew the capability within the Army. EW may need to part with past practices and redefine itself against today's operational environment. There is no reason EW cannot emerge in the next decade as a significant Army capability, but just as in the world of psychology, leaders must first admit there is a problem.

---

[80] American Psychiatric Association, *Diagnostic and Statistical Manual of Mental Disorders,* 4th ed. (Arlington, VA: American Psychiatric Association, 2000), 116-118.

Bibliography

Aid, Matthew M. *The Secret Sentry: The Untold History of the National Security Agency*. New York: Bloomsbury Press, 2009.

Air Force Technology. "F-16 Fighting Falcon Multirole Fighter." Accessed January 20, 2019. https://www.airforce-technology.com/projects/f16/.

American Psychiatric Association. *Diagnostic and Statistical Manual of Mental Disorders.* 4th ed. Arlington, VA: American Psychiatric Association, 2000.

Army Intelligence Center. *Student Text 2-50: Intelligence and Electronic Warfare (IEW) Systems*. Fort Huachuca, AZ: Army Intelligence Center, 2002.

Baker, Daniel. "Deep Attack: A Military Intelligence Task Force in Desert Storm." *Military Intelligence Professional Bulletin* 34-91–4 (December 1991): 39-42.

Behler, Robert F. *Director, Operational Test and Evaluation FY 2018 Annual Report*. Washington, DC: Government Printing Office, 2018.

Bigelow, Michael. "Short History of Army Intelligence." *Military Intelligence Professional Bulletin* 34-12–3 (September 2012): 7–69.

Blake, Bernard. *Jane's Radar and Electronic Warfare Systems: 1991-1992*. Coulsdon, Surrey, England: Jane's Information Group, 1991.

Bonnot, Douglas W. *The Sentinel and the Shooter*. Livermore, CA: WingSpan Press, 2010.

Brown, Duncan. "Last Gasp of the ASA." ASA Lives. Accessed January 22, 2019. http://www.asalives.org/ASAONLINE/lastgasp.htm.

Chalfant, Morgan. "Army Struggling to Fund Projects to Combat Electronic Warfare." The Washington Free Beacon, July 20, 2015. Accessed January 24, 2019. https://freebeacon.com/national-security/army-struggling-to-fund-projects-to-combat-electronic-warfare/.

Cohen, Eliot A. *Gulf War Air Power Survey, Volume IV: Weapons, Tactics, and Training and Space Operations*. Washington, DC: Government Printing Office, 1993.

Collins, Liam. "Russia Gives Lessons in Electronic Warfare." *Association of the United States Army*, July 26, 2018. Accessed January 24, 2019. https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare.

De Arcangelis, Mario. *Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts*. New York: Blandford Press, 1985.

EDO Corporation. "EDO Receives $86 Million Order for CREW 2.1 Counter-IED Systems." *Defense-Aerospace*, December 12, 2007. Accessed January 21, 2019. http://www.defense-aerospace.com/article-view/release/89132/edo-wins-$86m-for-counter_ied-systems.html.

Finnegan, John Patrick, and Romana Danysh. *Military Intelligence*. Washington, DC: Center of Military History, 1998.

Forecast International. "ALQ-151(V) (Advanced Quick Fix) - Archived 4/2000." Airborne Electronics Forecast, April 1999. Accessed January 20, 2019. https://www.forecast international.com/archive/disp_old_pdf.cfm?ARC_ID=32.

Frater, Michael R., and M. J. Ryan. *Electronic Warfare for the Digitized Battlefield*. Norwood, MA: Artech House, 2001.

Freedberg Jr., Sydney J. "Army Wrestles with SIGINT vs. EW." *Breaking Defense*, July 31, 2018. Accessed January 24, 2019. https://breakingdefense.com/2018/07/army-wrestles-with-sigint-vs-ew/.

"From Ravens to Prowlers." *Air Force Magazine* (August 1998): 76–81.

Godding, George A. "An InnerView of ASA as Seen by General Godding." *The Hallmark: United States Army Security Agency* 8, no. 8 (September-October 1975): 14-16.

Good Moring Science. "Electronic Warfare-The Future." October 9, 2017. Accessed January 20, 2019. https://gmsciencein.com/2017/10/09/electronic-warfare/.

Gordon, Don E. *Electronic Warfare: Element of Strategy and Multiplier of Combat Power*. 2nd ed. Oxford: Pergamon, 2014.

Government Accounting Office. *Electronic Warfare: Test Results Do Not Support Buying More Common Sensor Systems*. Washington, DC: Government Printing Office, 1998.

Keller, John. "SWaP: How Size, Weight, and Power Are Transforming the Military Electronics Industry." *Military and Aerospace*, June 1, 2013. Accessed January 20, 2019. https://www.militaryaerospace.com/articles/print/volume-24/issue-6/news/trends/swap--how-size--weight--and-power-are-transforming-the-military-.html.

Kofman, Michael, Katya Migacheva, Brian Nichiporuk, Andrew Radin, Olesya Tkacheva, and Jenny Oberholtzer. *Lessons from Russia's Operations in Crimea and Eastern Ukraine*. Santa Monica, CA: RAND Corporation, 2017. Accessed January 22, 2019. https://www.rand.org/pubs/research_reports/RR1498.html.

Lawlor, Maryann. "Signal Intelligence System Uncovers Enemy Sites." *SIGNAL Magazine*, October 2002. Accessed January 21, 2019. https://www.afcea.org/content/signal-intelligence-system-uncovers-enemy-sites.

Leonardo DRS. "Short History of US Army Electronic Warfare." Accessed January 21, 2019. https://www.leonardodrs.com/sitrep/q1-2016-the-invisible-fight/short-history-of-us-army-electronic-warfare/.

Lockheed Martin. "F-35 Electronic Warfare Capabilities." F-35 Lightning II. Accessed January 20, 2019. https://www.f35.com/about/capabilities/electronicwarfare.

Marine Corps System Command. "CVRJ CREW Fact Sheet." Accessed January 19, 2019. https://www.marcorsyscom.marines.mil/Portals/105/PMMC3/MC3PDF/2%201%20CVRJ%20CREW%20FACT%20SHEET.pdf.

Metternich, Ronald. "Counter-IED Road to War." National Training Center, December 2, 2007. Kenneth King Personal Records.

Mullin, Dustin. "Navy Growlers Train with Air Force, Marines during Red Flag 17-3." Nellis Air Force Base, July 26, 2017. Accessed February 7, 2019. https://www.nellis.af.mil/News/Article/1262522/navy-growlers-train-with-air-force-marines-during-red-flag-17-3/.

Office of the Director, Operational Test and Evaluation. "Prophet Report for the Office of the Secretary of Defense." 1999. Accessed January 20, 2019. http://www.dote.osd.mil/pub/reports/fy1999/pdf/army/99prophet.pdf.

Peterson, Kevin C. "Prophet Program Brief." IEW&S Program Executive Office, August 2001. Kenneth King Personal Records.

Pike, John. "AN/TLQ-17A(V), TRAFFICJAM." Federation of American Scientists. January 21, 1999. Accessed January 19, 2019. https://fas.org/man/dod-101/sys/land/an-tlq-17.htm.

Pomerleau, Mark. "For Better Electronic Warfare, the Army and Marine Corps Work Together." *C4ISRNET*, July 19, 2018. Accessed January 21, 2019. https://www.c4isrnet.com/electronic-warfare/2018/07/19/for-better-electronic-warfare-the-army-and-marine-corps-work-together/.

———. "How Will the Army Use Electronic Warfare? The Pentagon's Weapon Tester Wants to Know." *C4ISRNET*, February 5, 2019. Accessed February 7, 2019. https://www.c4isrnet.com/electronic-warfare/2019/02/04/how-will-the-army-use-electronic-warfare-the-pentagons-weapon-tester-wants-to-know/.

———. "New Electronic Warfare Program Tops Army Intel Wishlist." *C4ISRNET*, March 6, 2018. Accessed January 24, 2019. https://www.c4isrnet.com/electronic-warfare/2018/03/06/new-electronic-warfare-program-tops-army-intel-wishlist/.

Popovich, Michael, and Jonathan B. Slater. "Prophet Enhanced NMIB." Prophet Product Manager, March 20, 2014. Kenneth King Personal Records.

Price, Alfred. *The History of US Electronic Warfare, Volume 3, Rolling Thunder Through Allied Force, 1964-2000.* Alexandria, VA: Association of Old Crows, 2000.

———. *War in the Fourth Dimension: US Electronic Warfare, from the Vietnam War to the Present*. Mechanicsburg, PA: Greenhill, 2001.

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

Snow, Shawn. "The Corps Is down to One Final EA-6B Prowler Squadron." *Marine Corps Times*, May 30, 2018. Accessed February 7, 2019. https://www.marinecorpstimes.com/news/your-marine-corps/2018/05/16/the-corps-is-down-to-one-final-ea-6b-prowler-squadron/.

Stevens, Andrew. "Ground Crew Leader's Brief." Project Manager Signal Warfare Overview, October 22, 2005.

Streetly, Martin. *Jane's Radar and Electronic Warfare Systems: 2011-2012*. Alexandria, VA: Jane's Information Group, 2011.

US Army Intelligence Center of Excellence. "Major General George A. Godding Military Intelligence Hall of Fame Biography." Accessed January 21, 2019. https://www.ikn.army.mil/apps/MIHOF/biographies/Godding,%20George.pdf.

———. "U.S. Army Computer Network Operations-Electronic Warfare Proponent (USACEWP)." Slide Presentation, CW2 Christopher G. Nason Military Intelligence Library, Fort Huachuca, AZ, 2008.

US Department of the Army. *Army Doctrine Reference Publication (ADRP) 1-02*, *Operational Terms and Graphics*. Washington, DC: Government Printing Office, 2016.

———. *Army Training and Evaluation Program (ARTEP) 34-398-12-DRILL*, *Crew Drills for the AN/TLQ-17A(V)3 Trafficjam Countermeasures Set*. Washington, DC: Government Printing Office, 2004.

———. *Field Manual (FM) 3-0, Operations*. Washington, DC: Government Printing Office, 2001.

———. *Field Manual (FM) 100-5, Operations*. Washington, DC: Government Printing Office, 1982.

———. *TOE 34285L-CTH*, *Commander's TOE Handbook: Military Intelligence Battalion, Division.* Washington, DC: Government Printing Office, 1990.

US House of Representatives. *Intelligence Successes and Failures in Operations Desert Shield/Storm*. Report of the Oversight and Investigation Committee on Armed Services. Washington, DC: Government Printing Office, 1993.

Van Pool, J. Elise. "CREW: Helping Defeat IEDs." *US Army*, October 26, 2011. Accessed January 21, 2019. https://www.army.mil/article/67963/crew_helping_defeat_ieds.

Weinstein, Sidney T. "Evolution of Military Intelligence." Memorandum for Military Intelligence Personnel, Fort Huachuca, AZ, January 3, 1984. Kenneth King Personal Records.

Wheeler, James Scott. *The Big Red One: America's Legendary 1st Infantry Division from World War I to Desert Storm*. Lawrence, KS: University Press of Kansas, 2007.