REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
05/15/2020	Master's Thesis	Aug 2019 - May 2020

4. TITLE AND SUBTITLE
EVOLVE OR DIE: ENHANCING ELECTRONIC WARFARE CAPABILITY IN U.S. ARMY BRIGADE COMBAT TEAMS TO MAINTAIN LETHALITY AND SURVIVABILITY IN COMBAT

5a. CONTRACT NUMBER
n/a

5b. GRANT NUMBER
n/a

5c. PROGRAM ELEMENT NUMBER
n/a

6. AUTHOR(S)
Lucas, Sean P.
Lieutenant Colonel, U.S. Army

5d. PROJECT NUMBER
n/a

5e. TASK NUMBER
n/a

5f. WORK UNIT NUMBER
n/a

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Joint Advanced Warfighting School
7800 Hampton Blvd.
Norfolk, VA 23511-1702

8. PERFORMING ORGANIZATION REPORT NUMBER
n/a

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Defense University
Joint Forces Staff College
7800 Hampton Blvd.
Norfolk, VA 23511-1702

10. SPONSOR/MONITOR'S ACRONYM(S)
NDU-JFSC

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

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution is unlimited

13. SUPPLEMENTARY NOTES
Not for Commercial Use without the express written permission of the author

14. ABSTRACT
The United States Army is not prepared to effectively operate in a contested electronic warfare (EW) environment while engaging in armed conflict against a peer adversary. In 2014 the Russian Army demonstrated their ability to rapidly locate Ukrainian command posts, front line combat formations and logistics support bases; to employ EW to defeat incoming artillery and mortar fire; to disrupt or deny Ukrainian communications; and to spoof or jam global positioning system receivers. This change in capability was unprecedented and caught the US military by surprise. The US Army must evolve or will suffer a similar fate if engaged in direct conflict with a peer adversary.

15. SUBJECT TERMS
Electronic Warfare, New Generation Warfare, Electronic Equipment, Hybrid Warfare

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Sean P. Lucas
					19b. TELEPHONE NUMBER *(Include area code)*
UNCLASS	UNCLASS	UNCLASS	Unclassified Unlimited	51	757-443-6301

NATIONAL DEFENSE UNIVERSITY

JOINT FORCES STAFF COLLEGE

JOINT ADVANCED WARFIGHTING SCHOOL

EVOLVE OR DIE: ENHANCING ELECTRONIC WARFARE CAPABILITY IN U.S. ARMY BRIGADE COMBAT TEAMS TO MAINTAIN LETHALITY AND SURVIVABILITY IN COMBAT

by

Sean P. Lucas

Lieutenant Colonel, United States Army

THIS PAGE INTENTIONALLY LEFT BLANK

EVOLVE OR DIE: ENHANCING ELECTRONIC WARFARE CAPABILITY IN U.S. ARMY BRIGADE COMBAT TEAMS TO MAINTAIN LETHALITY AND SURVIVABILITY IN COMBAT

By

Sean P. Lucas

Lieutenant Colonel, United States Army

A paper submitted to the Faculty of the Joint Advanced Warfighting School in partial satisfaction of the requirements of a Master of Science Degree in Joint Campaign Planning and Strategy. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Joint Forces Staff College or the Department of Defense.

This paper is entirely my own work except as documented in footnotes.

Signature: Sean P Lucas

15 May 2020

Thesis Advisor:

Signature: Homer Harkins

Homer Harkins, Ed.D., Professor
Joint Special Operations University

Approved by:

Signature: for Miguel L. Peko

Michael Bennett,
Special Operations Academic Chair,
Committee Member, Joint Advanced Warfighting School

Signature: Miguel L. Peko

Miguel L. Peko, Captain, U.S. Navy
Director, Joint Advanced Warfighting School

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Army is not prepared to effectively operate in a contested electronic warfare (EW) environment while engaging in armed conflict against a peer adversary. In 2014 the Russian Army demonstrated their ability to rapidly locate Ukrainian command posts, front line combat formations and logistics support bases; to employ EW to defeat incoming artillery and mortar fire; to disrupt or deny Ukrainian communications; and to spoof or jam global positioning system receivers. This change in capability was unprecedented and caught the US military by surprise.

The US Army is currently minimally manned and poorly equipped to conduct offensive or defensive EW operations, cannot effectively locate or track adversarial communications and cannot effectively defend itself from adversarial attacks. The US Army needs to conduct immediate evolutionary change to EW equipment available within brigade combat teams while increasing the manning levels to provide offensive and defensive capability at the company, battalion and brigade levels. This enhanced capability will ensure that US formations are not overmatched by peer adversaries on the modern battlefield. Additionally, the US Army needs to invest in researching technology and systems that will provide long term revolutionary change in how EW is waged and the degree with which it can be employed.

Without immediately addressing the gaps in electronic warfare that currently exist between US formations and peer adversaries, the US risks being outmaneuvered and incurring unacceptable levels of casualties on the modern battlefield. Systems currently exist in the US inventory and technology exists in friendly and adversarial militaries that should be harnessed to close the current capabilities gap.

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Introduction

After eighteen years of continuous conflict and the optimization of military formations for the conduct of counterinsurgency operations in concert with wide area security, the U.S. Army's ability to dominate in land warfare has atrophied. Technological advancements have been curtailed, combined arms maneuver has become a secondary task and the growth of adversarial capability has gone unchecked.[1] In February 2014 Russia invaded Eastern Ukraine and demonstrated a new generation of warfare. Not massed regiments and divisions fighting along large fronts but smaller brigade sized tactical formations fighting with precision, massed fires, and the disruption of the entire electromagnetic spectrum. Electronic warfare (EW) was seamlessly synchronized with unmanned aerial systems and long-range fire support.[2] This form of warfare was unexpected, the level of electronic disruption was unprecedented, and the United States was unaware that Russia had the ability to operate with that degree of precision.

The critical component to the Russian success was their EW capability. Without interruption they were able to collect intelligence on Ukrainian positions, locate tactical formations and operations centers, disrupt communications, seed unrest and destroy critical Ukrainian capabilities. They demonstrated an ability to mass effects at the time and location of their choosing and dominate their adversary across the battlespace.[3] The U.S. Army, though larger and more capable than the Ukrainian Army, does not possess a

[1] These assertions are based on the author's personal observations and experiences, though they are well documented by multiple sources as an assessment on the re-emergence of great power competition.
[2] Liam Collins, "Russia Gives Lessons in Electronic Warfare," *Association of the United States Army*, July 26, 2018, https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare (accessed November 10, 2019).
[3] Daniel Brown, "Russian-backed separatists are using terrifying text messages to shock adversaries — and it's changing the face of warfare," *Business Insider,* August 14, 2018. Paraphrase of the article.

greater capacity to counter this form of fire and maneuver, synchronized with electronic effects.

The modern-day battlefield has changed and victory cannot be assumed by the nation with the largest military and most powerful weapons. With the increase in EW capability in the Russian Army and technology that has been fielded to brigade tactical formations, the Russian Army may have gained a marked advantage over similar sized formations in the U.S. military. [4]

The thesis of this research is that the U.S. Army currently lacks the organization, personnel, and equipment within tactical formations necessary to optimize lethality and survivability on the modern battlefield against a peer enemy. The U.S. Army must develop new EW systems while increasing personnel manning to develop an offensive and defensive EW capability at the Brigade level and below. This organization should include enhanced intelligence collection and targeting capability, detection and protection from threat EW attack, and the ability to conduct electronic attack (EA) at the discretion of the commander. [5]

Research on this topic will include a study on Russian operations in Ukraine to build a deeper understanding of Russian capabilities. By studying operations in Ukraine, technologies and procedures for how EW was used, how it supported other operations, and how it was used as a targeting capability itself will be gained. This will help define the capabilities that a peer adversary possesses and enable a comparison to U.S. capability. The next area for research will be on current U.S. EW capability within

[4] This is an assumption by the author that will be analyzed throughout the thesis.
[5] The author will argue that the U.S. Army must match or overmatch Russian capability or run the risk of tactical defeat at the brigade level and below.

tactical formations. Focus will be on the brigade combat team, as that is the unit of action for direct combat within Army formations, and the technology and task organization that currently exists to support offensive and defensive EW. The final area for study will be on emergent technologies and capabilities that currently exist that can provide immediate enhanced capability to U.S. Army formations. After building an understating of Russian and U.S. capability, a comparison can be made and recommendation provided to support growth in personnel and enhancements in equipment to facilitate the maximization of U.S. ground force lethality.

The research will focus on the brigade level to allow comparison between like-sized units in the Russian and U.S. Army. Joint force enablers, specifically from the U.S. Air Force and Navy, will not be included in the study as there are limited numbers of platforms available and there can be an assumption of land operations being conducted in areas where airspace is contested and aerial EW platforms are unable to operate. Classified capabilities and emergent technologies will not be explored nor will signals intelligence and EW capability in U.S. Special Operations Forces be included unless there is a direct link to brigade combat teams or future plans for fielding across the general-purpose forces.

The U.S. Army must remain capable of conducting combined arms maneuver as part of a widespread ground conflict. If potential adversaries have the capability to actively gain intelligence on and target U.S. forces using electronic warfare means, the U.S. Army will be at a disadvantage and will assume a degraded comparative strength.[6] Through the study of demonstrated Russian and current U.S. Army capabilities, a shortage in trained

[6] Relative strength between the Russian and U.S. Military will not be explored as a macro comparison. The relative strength will be an analysis of how formations are using and enhancing EW for tactical advantage.

personnel and adequate equipment will be identified within U.S. formations. Through the comparison of like sized units, the reader will gain an appreciation of the need to change the organization, manning, and equipping within U.S. formations to allow a competitive advantage over peer adversaries.

Ukraine 2014: Demonstrated Russian Electronic Warfare Capability

This chapter will demonstrate a capability that currently exists within the Russian military to conduct electronic warfare (EW) as part of multi domain conflict. The chapter will explore the capabilities that were observed and assumed during the invasion of Eastern Ukraine in 2014 and how EW was used to maximize the precision and effectiveness of Russian operations. Ultimately, the chapter will use the context of demonstrated Russian capability as a threat that the U.S. military needs to be able to counter.

In February 2014 Russia began offensive military operations in Eastern Ukraine to seize control of critical terrain and infrastructure and ensure Russian strategic interests would be met in the years ahead.[7] This operation, though unexpected and without warning, was not out of step with historic Russian aggression and methods for exertion of power and influence. What appeared atypical was the efficiency and precision with which they conducted the attack. The Russian military's ability to influence a population, to seed discontent, to mass fires at a precise moment and to disrupt Ukrainian electronic systems demonstrated a level of precision and capability that far exceeded NATO assessments and United States capacity to counter.[8]

Demonstrated Russian Electronic Warfare Capability

Since Russian operations began in Ukraine in 2014 Russia has continuously used and refined tactics, techniques and procedures for the employment of EW. From initial shaping operations at the onset of conflict through the use of advanced technologies and

[7] Headquarters, United States Army Special Operations Command, *Little Green Men: a Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014* (Fort Bragg, NC: United States Army Special Operations Command, 2016), 37-39.
[8] *Little Green Men*, 53-61.

systems in the current day, Russia has continuously employed and refined the use of EW to disrupt Ukrainian systems and target Ukrainian forces while ensuring their own maneuverability within the electronic domain.[9]

Russian front line military units have been able to synchronize the use of ground and aerial electronic collection assets with unmanned aerial systems (UAS) to collect electronic intelligence while simultaneously overlaying it with full motion video.[10] Though this technology is not entirely unique to the Russian military, the extensive use by forces at multiple echelons can be assumed to mean that there has been a proliferation of training and technology across their formations.

Russia uses EW for four principle reasons and has the ability to synchronize the actions or intelligence collected through electronic means with kinetic effects. The four principle roles are:

1. Denying communication.
2. Defeating unmanned aerial systems.
3. Defeating artillery and mortars.
4. Targeting command and control nodes.[11]

By synchronizing these effects with kinetic fires and maneuver or in concert with subversion or special operations missions, the Russian military has the capability to deny, disrupt or destroy their adversary's ability to command and control operations,

[9] Liam Collins, "Russia Gives Lessons in Electronic Warfare," *Association of the United States Army*, July 26, 2018, https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare (accessed November 10, 2019).
[10] Collins.
[11] Philip Karber, "Russia's New Generation Warfare," *Association of the United States Army,* May 20, 2016, https://www.ausa.org/articles/russia%E2%80%99s-new-generation-warfare (accessed October 18, 2019).

communicate with adjacent units or collect intelligence and maneuver against Russian formations.

Technology possessed in the Russian Army allows them to deny communications across wide spectrum electromagnetic bands, effectively shutting down all cellular, line of sight and video communications networks. This was apparent at the onset of hostilities in Ukraine and still exists today in large regions in Donbass.[12] Communication between units, passing of orders through echelons of command, distribution of media to the population and maintaining situational awareness of enemy actions can be denied through the disruption of electromagnetic systems. Without the ability to communicate, military formations will be forced to operate blindly; Russia has demonstrated the ability to deny their enemy use of communications while simultaneously maneuvering throughout the social and physical terrain.

Unmanned aerial systems (UAS) have been promulgated across the battlefield by a vast majority of militaries across the world, including the United States. UAS are used for reconnaissance, surveillance, intelligence collection, and to conduct kinetic strikes. Russian EW capability can either deny UAS employment or defeat their use once airborne. As the conflict in Ukraine began, the single most capable asset employed to defeat Ukrainian UAS was EW, destroying more UAS than all other systems combined.[13] Through the defeat of the Ukrainian UAS capacity, Russia essentially prevented effective reconnaissance of their positions and collection of their electronic signature. This provided them the necessary maneuver space and time, without compromise, to position

[12] Karber.
[13] Karber.

their artillery and maneuver forces on the battlefield where they could most rapidly defeat Ukrainian formations.

Communication is essential to successfully employing indirect fires, establishing the link between the observer that sees the enemy and the shooter that will employ the weapons systems. This link can be broken through communication denial, an effective means to prevent accurate fire support, but a lesser known capability exists to defeat the artillery and mortar rounds themselves once fired. Rounds that are fired with electronic fusing, specifically proximity or guided munitions, can be prematurely triggered or forced to dud through electronic means.[14] Though not widespread and reactionary in nature, Russia demonstrated the capability to employ this technology in Ukraine, essentially denying communication between the observers and firing unit and subsequently defeating the rounds once fired. New Russian EW systems have the ability to confuse incoming artillery and missiles and overload guidance modules; rendering some guided missiles useless or degraded.[15]

Mission Command nodes and headquarters have been a focus of attack for offensive military operations throughout history and it is well documented that defeating the enemies' ability to plan, coordinate and synchronize operations can lead to rapid victory or change the tide of conflict. History has also proven that locating the enemy command nodes is a much greater challenge that defeating it once located. Ground and aerial reconnaissance occasionally yields success in locating enemy headquarters, but electronic reconnaissance and monitoring has proven to be significantly more effective when

[14] Karber.
[15] Asymmetric Warfare Group, *Russian New Generation Warfare Handbook,* Version 1 (Washington DC: Asymmetric Warfare Group, December 2016), 9.

properly used. Russian EW reconnaissance systems allow for the near real time understanding of enemy positions, across the battlefield, through the monitoring of radio, cellular and satellite signals.[16] Without a need to fully understand what information is being passed, the signals collected can easily identify locations and the nature of the signals can help identify what type of unit or headquarters is positioned there. With the locational data on enemy mission command nodes, the massing of fires against those targets has proven decisive to rapid victory.

Russian EW capability has been seen throughout the conflict in Ukraine. It has provided Russia with a marked advantage over their adversaries through the denial of UAS, the defeat of all forms of electronic communications, disruption of fire support capability and near perfect understanding of command and control nodes on the battlefield. The extensive use of electronic warfare was something that Ukraine was not prepared to counter and presents the United States with an updated understanding of expanded Russian capability.

Gerasimov Doctrine and Russian New Generation Warfare

In 2013 General Valery Gerasimov, the Russian Chief of the General Staff, published an article in the Russia trade paper *Military-Industrial Kurier* that outlined his vision for employment of military power. His description of conflict not involving massed military formations and instead using subversion, deception, political unrest and protest as the major form of maneuver was groundbreaking and presented the idea that struggle is continuous. It introduced new problems for cyber security, new ideas for political gain and popular support and new concepts for the use of electronic warfare. Much of the

[16] Karber.

Gerasimov Doctrine, as it has been coined, involves the use of electronic and cyber warfare capability to influence the political and social opinions of enemy or potential enemy populations. This thesis will not explore those aspects but will instead focus on the doctrine and how EW can be used as part of combined arms on the kinetic battlefield.

Hybrid warfare, as the United States refers to it, or non-Linear warfare, as the Russian call it, refers to conflict being a combination of conventional, irregular and cyber threats operating seamlessly and in concert across all domains on the battlefield.[17] Electronic Warfare is a major component to that. EW on the battlefield is used to influence adversaries to maneuver, to garner a communications response, or to change perspective or morale of a formation. Russian operations in Ukraine demonstrated the ability to do all of these things, through the denial of communications systems or introduction of signals that presented a different perspective than the Ukrainian soldiers believed to be true.

Russian EW systems have demonstrated the ability to directionally find enemy positions and determine the composition of that position through the nature of the signals. Additionally, they have shown the ability to collect cellular information for the individuals in a certain area and communicate to those devices at their discretion. This overlaying of signals intelligence through the conduct of electronic warfare has proven to be decisive to effective employment of fires and to degrade morale of adversaries. In Ukraine, Russian EW assets were able to detect Ukrainian signals and conducted massed artillery strikes on the location. This action in itself is not historically significant, but the Russian command followed the artillery strike with text messages to the Ukrainian

[17] Joshua Stowell, "What is Hybrid Warfare?" *Global Security Review,* August 1, 2018, 5.

soldiers asking them about the artillery strike and inquiring about how effective it was. This was followed up by additional artillery fire.[18]

The ability to collect electronic signals, determine composition and strength of the enemy at the position, conduct massed artillery and rocket fire while simultaneously communicating with the soldiers receiving the fire to degrade morale is the fusion of electronic, kinetic and psychological effects that Gerasimov had alluded to.

Soon after the invasion of Ukraine, Major General Yuriy Lastochkin, the commander of Russian EW forces noted:

> There is nothing surprising that in the current circumstances, EW—as a relatively inexpensive and easily implemented means to disrupt the functioning of an enemy's radar and other systems and to defend one's own similar systems from interference—is emerging as a priority and a focus for development. In certain circumstances, use of EW approaches can be viewed as asymmetric measures that negate the benefits of an adversary's highly sophisticated systems and means of armed combat.[19]

Russia had clearly been building its EW capability and reinforcing technology that was both militarily effective and fiscally responsible. The Russian military complex had developed a new concept for waging war and had started to build the technology to support the doctrine years in advance. Electronic systems could negate the advantages of much more expensive, technologically superior systems through the denial of communication or navigation. The United States was not expecting to see this.

Maneuver forces in the Russian Army are equipped with EW capability that allows them to conduct operations that have tactical, operational and potentially strategic impacts on their enemy. At the maneuver brigade, they have equipment that can effectively spoof Global Positioning System (GPS) locational data, deny use of satellite

[18] *Russian New Generation Warfare Handbook,* 13.
[19] Roger N. McDermott, "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum," *International Centre for Defense and Security*, September 2017, 3.

communications, directionally find electronic emissions, disrupt precision guided munitions and deny terrestrial based communications.[20] With the emphasis on combined arms in the new generation warfare, Russian maneuver brigades have the capability to rapidly link their EW collection with fires assets and employ long range fires to destroy an identified adversary. Without requirement for higher echelon assets, Russian brigades can deny high frequency (HF), very high frequency (VHF), ultra-high frequency (UHF), cellular, INMARSAT/IRIDIUM, and satellite communications.[21] Additionally brigades have the ability to deny airborne and ground based early warning systems and deny airspace to UAS. This capability, at the lowest tactical level, give Russian maneuver commanders the flexibility to target adversarial nodes and formations with precision and expedience.

New Generation Warfare wages battle in all domains. The doctrine and equipment used by the Russian military to wage this form of war already exists and has been validated on the battlefield. EW collection, synchronized with the employment of fires and overlaid with the psychological effect of harassment through cell phones has proven to be critical to Russian victory in Ukraine. These evolving concepts are inexpensive relative to advanced weapons and may cripple a larger, more technologically advanced adversary.

Vulnerability in United States Systems

The United States military has enjoyed years of relative security for headquarters elements, operated in non-denied airspace, has been unencumbered by electronic

[20] Lester Grau and Charles Bartles, *The Russian Way of War* (Fort Leavenworth: Foreign Military Studies Office, 2016), 289.
[21] Grau, 292-297.

signature and could target adversaries on the battlefield of Iraq and Afghanistan through electronic means with relative ease. Fighting an enemy that did not possess advanced offensive or defensive EW capability brought an unwarranted sense of calm to the idea that the U.S. maintains electronic dominance. That may not be the case anymore. Battalion level and higher headquarters are slow to move, have large electronic and visual signatures and can be located with ease by adversaries who have advanced EW directional finding capability. U.S. commanders are accustomed to receiving continuous updates from subordinate formations and leaders, have become reliant on over communication of ideas and control of situations and make a habit out of maintaining constant contact up, down, and across the chain of command.[22] This reliance on systems that emit large electronic signatures, on technology that can be jammed or spoofed and with limited ability to detect jamming or counter its effects may put U.S. forces at risk of destruction in future conflict.

The U.S. Army relies on archaic mission command systems that use large amounts of bandwidth, GPS locations and satellite communications. These systems can be disrupted during major combat operations if space is a contested domain and communications satellites are not reliable or functional, during regional conflict if GPS systems are jammed or spoofed and during any conflict if the adversary has the capability to directionally find forces on the battlefield through the interrogation of its electronic signal.[23]

[22] This is an assessment by the author based on personal experience and observations.
[23] Andrew Boyd, "Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army," *The Institute of Land Warfare*, November 2017, 18.

With the presence of Russian EW systems at almost every echelon, the U.S. Army is vulnerable to the effects of electronic attack, reconnaissance and jamming. The United States does not currently employ EW is mass at lower level formations; certainly not down to the company and battalion level. This inability to counter Russian EW targeting and overreliance on electronic data exposes U.S. formations to similar kinetic effects that have plagued Ukrainian forces during their 5 year conflict with Russia.

Vulnerabilities exist in U.S. systems to electronic attack and disruption but the greatest threat to U.S. ground forces resides with the reliance on technology and communications to manage the battlefield and a seemingly insatiable appetite for information and connectivity.

Chapter Summary

The Russian military surprised the world in 2014 when it invaded Eastern Ukraine. The geopolitical maneuvering was unexpected but the brutal efficiency with which they attacked, the effectiveness and precision of their targeting and the inability of the Ukrainian army to counter the Russian advance was revolutionary. The Russian military had demonstrated the effectiveness of electronic warfare and how it possessed the ability to precisely locate adversarial communications, jam or spoof GPS locations, conduct information operations through sending fake text messages to Ukrainian soldiers, deny and destroy unmanned aerial systems, and mass indirect fires and rockets against positions identified by their electronic signature. Combined arms maneuver and the precision of attack had rapidly evolved and the United States was unaware that it was happening.

The U.S. relies heavily on communications, connectivity and information at every level. From a team radio to tactical operations centers, the U.S. military presents significant vulnerabilities to EW targeting by Russian forces or forces equipped with Russian technology. The next chapter will explore the current capabilities and technology that resides within U.S. Army brigade combat teams and identify gaps in manning and equipping that present vulnerabilities to the capabilities that have been observed within Russian formations.

Electronic Warfare Capabilities and Gaps in U.S. Army Brigades

The United States Army is built for one purpose – to fight and win the nations wars. It has been optimized to engage in major land combat and win decisive battles on behalf of the American people. Combined arms maneuver, air-land battle, synchronization of assets across time and space, delivering maximum destructive effects on the enemy while exposing the least number of Americans to danger are what have defined the American way of war for the past 50 years.

Those times have changed. The U.S. military is faced with challenges that curb the way America will wage war. Gone are the days of guaranteed communications; gone is the luxury of security for static headquarters; gone is the ability to mass fires without fear of detection. The U.S. military, specifically the Army, must be manned and equipped to fight a new type of land warfare. It must have the personnel trained to detect enemy electronic warfare attacks, locate enemy nodes and deny enemy the use of the cyber and electronic domains. To understand what capability currently resides within the Army, analysis of personnel manning and equipping must be done.

Once an appreciation of manning and equipment capabilities is developed, the gaps between U.S. and Russian battlefield advantage can be explored.

Manning of Electronic Warfare Specialists in Tactical Formations

The U.S. Army is manned with electronic warfare personnel at every echelon, from battalion to theater Army. Their duty positions range from cyber electronic warfare officer (CEWO), electronic warfare technician, electronic warfare noncommissioned officer, spectrum manager and battalion electronic warfare personnel.[24] These duty

[24] Headquarters, Department of the Army, *Electronic Warfare Techniques,* Army Techniques Publication 3-12.3 (Washington DC: US Government Printing Office, 2019) 2-1 through 2-5.

positions are filled at each echelon, but the focus of study will be at the brigade combat team (BCT) level to facilitate a comparison to Russian manning and capabilities in maneuver brigades. In exploring the duties of each position, an understanding of capabilities and expectations can be established.

The Brigade Cyber Electronic Warfare Officer (CEWO) is overall responsible for the synchronization and coordination of EW effects and operations across the BCT area of operation. This includes nominating EW targets to the fire support coordinator and commander, prioritization of EW assets, and processing targets for subordinate elements.[25] The Electronic Warfare Technician is the subject matter expert for the employment of EW assets across the BCT and maintains the adversarial electromagnetic survey for the BCT area of responsibility.[26] The Electronic Warfare Noncommissioned Officer plans and executes the EW tasks as defined in the orders process for the BCT and manages the availability of EW tools and equipment.[27] The Spectrum Manager is responsible for synchronizing the EW plan to ensure there is no degradation to friendly force emitters or systems and protects the integrity of radio frequency and cyber linkages.[28]

The total number of soldiers working in the EW section at the BCT level is four. There are no personnel who are assigned to collect electronic intelligence or develop electronic attack opportunities to degrade enemy capabilities. None of the duty descriptions, for any of the personnel within the BCT headquarters are tasked to collect; they are all tasked to synthesize what is collected through other means and from the joint

[25] Army Techniques Publication 3-12.3, 2-1.
[26] Army Techniques Publication 3-12.3, 2-2.
[27] Army Techniques Publication 3-12.3, 2-2.
[28] Army Techniques Publication 3-12.3, 2-3.

force. This clearly identifies a gap in focus for the brigade and limits what can be done to support EW targeting. The manning at the battalion level is even less.

Within a maneuver battalion, as part of a brigade combat team, there is one assigned electronic warfare specialist. The role of the battalion EW specialist is to plan and integrate EW capabilities into battalion operations and pass requests for support to the brigade EW team.[29] There are no assigned EW collection specialists or individuals trained to identify and deny enemy electronic attack or monitoring.

The military intelligence company, resident within the brigade engineer battalion, as part of a BCT has intelligence collection capability and platoons. The company is organized into four platoons: analysis, signals intelligence, human intelligence and unmanned aerial systems.[30] The capability of these platoons varies and the signals intelligence (SIGINT) platoon is only manned with 8 personnel. SIGINT capacity within the company is limited to two platforms, both of which must operate in close proximity to the other while neither can provide long range signals intercept. The general concept for employment is to maneuver both teams forward with either infantry or cavalry platoons to provide limited collection of SIGINT to satisfy information requirements for the brigade commander. Though capable and trained to execute these tasks, they are limited in both depth and breadth of collection.

The manning of EW personnel across the BCT is minimal and does not represent a focus on the conduct of EW operations in an environment where the electromagnetic spectrum is contested. Various U.S. Army units have explored different task

[29] Army Techniques Publication 3-12.3, 2-3.
[30] Headquarters, Department of the Army, *Brigade Combat Team*, Field Manual 3-96 (Washington DC: Department of the Army, October 2015), 1-6.

organizations to maximize EW capability, using the current manning and equipping available, but none have been optimized for success against a peer adversary. The 173rd Airborne Brigade conducted extensive EW testing and evaluation to determine if EW could be maximized by consolidation of personnel into one platoon and employment as an intelligence collection asset. The results were positive, but micro in scope.

In February 2018 the 173rd directed the consolidation of SIGINT collection assets from the military intelligence Company with EW specialist from all of the maneuver battalions. This allowed them to form a Combat Electronic Warfare Intelligence (CEWI) platoon manned with eight soldiers.[31] The capability that this platoon provided proved to be extremely beneficial, but small in scope. As a test bed for further evaluation and analysis, it appears to have provided concepts for employment of EW collection and targeting assets, but the scale to which it was employed and the impact that it had on the fight beyond benefiting one reconnaissance troop was minimal.[32] The platoon, using newly fielded equipment, was able to identify local enemy signatures and assist with ground or aerial reconnaissance of those positions. Unfortunately, due to the minimal manning available and inability to cover the entire battlespace of the BCT, they were unable to locate, assess or destroy enemy critical capabilities or assets.

Shortcomings exist within the BCT to effectively collect signals and maximize friendly capability to conduct electronic warfare. The minimal manning of personnel at the battalion level and below and of signals intelligence specialists within the SIGINT

[31] Doni Wong, Theodore Lipsky, Briged Calhoun and Pablo Cruz, "Integration of Signals Intelligence, Electronic Warfare in Reconnaissance Troop: Seeing Where the Eye Cannot See," *Armor Magazine*, Fall 2018, 13-19.
[32] Wong, 18.

collection platoon severely degrades the BCTs ability to locate, assess, characterize and engage enemy critical capabilities using EW.

Current Electronic Warfare Equipment Fielded to the U.S. Army

In looking at the capability for tactical formations to conduct electronic warfare, building an understanding of the technology and equipment that is currently fielded will inform a comprehension of the effectiveness of those units. Acknowledging that there isn't the manning required to support EW operations within battalions, the focus will reside on the military intelligence company, the enhanced capability that was introduced with the formation of the CEWI platoon and the resident systems at the BCT level to synthesize the intelligence gathered with organic and external EW collection platforms.

The military intelligence company is equipped with two primary systems to collect and directionally find enemy signals. They are the prophet and the low-level voice intercept (LLVI) systems. There are two of each system in the company and they represent the entirety of a BCTs ability to listen to and locate enemy signals and communications.

The Prophet system is a vehicular mounted signals collection platform that provides static and on-the-move passive collection of adversarial signals and has the ability to triangulate the location to within a few hundred meters. This capability provides an invaluable advantage to U.S. Army BCTs when properly employed and allows commanders to make decisions about force protection and offensive operations. The system can be dismounted from the vehicle and operated in a degraded mode for short duration missions. Though capable, the range for collection is limited and it requires line of sight to the emitter to effectively listen to the transmission and must be within a

narrow bandwidth to effective directionally find it. This information can inform decisions by commanders but does not provide long range signals intercept that can be used effectively to target major enemy formations or capabilities.

The Low Level Voice Intercept (LLVI) is a man portable system that has similar characteristics to the Prophet, but in a man portable and smaller configuration. The LLVI team, consisting of two personnel, typically deploys forward as part of a reconnaissance or maneuver force to gather intelligence about enemy personnel near the forward line of own troops (FLOT). The LLVI team assists the unit it is collocated with by identifying possible enemy positions, information about enemy movement and provides early warning about enemy attacks. The LLVI is limited by range, mobility and breadth of coverage. The ability to conduct EW forward of the FLOT is very limited and the system has proven to be most useful in providing early warning of pending enemy actions.[33]

The ability of the brigade EW cell to synthesize the intelligence gathered across the battlespace by the limited sensors available is critical to the ability of the BCT to conduct offensive or defensive operations using the signals and electronic intelligence that is gathered. The BCT CEWO uses the Electronic Warfare Planning and Management Tool (EWPMT) to compile all available electronic warfare inputs and develop an EW common operational picture (COP) for the commander and staff to use.[34] This information is valuable for decision making and targeting but the limited amount of ground sensors on the battlefield and limited access to joint aerial enablers provides for a relatively sparsely populated EW COP. The system allows for immediate action between the CEWO and the fires support coordination officer in the BCT operations center if a target is identified but

[33] Interview with a Military Intelligence Company Commander, 24 October 2019.
[34] Army Techniques Publication 3-12.3, C-1.

in practice the amount of actual capability to detect is limited and prohibits effective targeting.[35]

Technology continues to evolve and the ability to effectively employ the tools that are available is becoming more ingrained in Army leaders as it becomes more routine to encounter EW on the battlefield. As the testing of the initial CEWI platoon was conducted by the 173rd in February 2018, the unit fielded the Versatile Radio Observation and Detection (VROD), VROD Modular Adaptive Transmit (VMAX), Saber Fury (a system designed to manage the EW environment), and Raven Claw (a system designed to be used with EW planning tools) to enhance their capability.[36] These systems proved to enhance the ability of the unit to conduct intelligence gathering and limited jamming but the range for employment and ability to detect critical enemy nodes was limited. The size of the CEWI platoon limited the depth and breadth of coverage and the systems typically provided information that was valuable to the maneuver units in the immediate vicinity but did not satisfy information requirements demanded by higher level commanders.

The technology that is fielded to U.S. Army maneuver forces, specifically at the brigade level, does not provide significant capability to execute EW operations in the offense or defense.

Shortfalls in Electronic Warfare Capability

Based on the manning and equipping shortfalls that have been identified, the U.S. Army does not possess the ability to conduct offensive or defensive EW at the BCT level. The current structure allows for the manning of four EW teams within the BCT, each

[35] Interview with a BCT CEWO, 28 October 2019.
[36] Wong, 13-19.

with the ability to collect signals for exploitation and directional finding, within close proximity to itself, but lack the ability to conduct electronic attack or jamming.

While conducting offensive operations, the BCT commander is tasked to synchronize effects from organic and inorganic assets to impose his will upon the enemy. Offensive operations are characterized by capitalization on accurate and timely intelligence about the enemy.[37] Traditional methods for gathering intelligence on the enemy continue to prove to be effective, but lacking a robust capability to gather real-time information on enemy movements, headquarters locations, plans and fires can significantly degrade the commander's ability to impose his will. Without knowing where the enemy is located and what his intentions are will increase the risk of chance contact with the enemy and decrease the capability to win a decisive battle.

The U.S. Army's ability to conduct defensive EW operations is very limited. With the minimal manning that currently exists in tactical formations and equipment that is used primarily to collect signals intelligence, BCTs lack the capability to understand when they are being targeted using electronic means and lack the experience necessary to counter those actions.[38] Despite significant changes being implemented through training at places like the National Training Center and Joint Readiness Training Center, units still lack the ability to mass their defenses against adversarial EW threats. With the promulgation of adversarial EW assets across the battlefield, the U.S. Army is significantly disadvantaged by not having organic EW detection and counter-EW capability in tactical formations. This presents a vulnerability to enemy action.

[37] Field Manual 3-96, 6-1.
[38] This is an assessment by the author based on personal observations and experiences.

Electronic attack (EA) is conducted in both the offense and defense and enables the commander to dominate the electromagnetic spectrum and support the friendly scheme of maneuver. The principle purpose is to affect enemy communications and can be used as an action in itself or as part of a lethal targeting process.[39] The U.S. Army relies on airborne EA capabilities and assets and does not have personnel or equipment within tactical formations that can conduct immediate, directed, or dynamic EA targeting. This limitation significantly degrades a BCT commander's ability to disrupt or deny enemy capability and may degrade the formations capacity to dominate an adversary.

The U.S. Army lacks the necessary personnel and technology to effectively conduct EW at the BCT level and it presents a risk to mission and force while engaging in conflict with an adversary with peer-like technology. The shortfall lies in both the number of personnel assigned to the brigade and the equipment that they use. EW is necessary across the breadth of the brigade area of operations and must extend deep beyond the FLOT. The current manning and equipping within the BCT prevents either of these requirements from being met.

Capability must be developed and fielded and manning must be enhanced to fill the gaps that are evident during training and operational deployments to ensure that U.S. Army BCTs maintain the ability to find, fix and finish enemy nodes and formations while ensuring that their adversary cannot do the same to them.

Divergent EW Equipment Capabilities between the U.S. and likely Adversaries

The stark contrast between the capability of the U.S. Army combat brigades and those of the Russian Army presents a divergence in electronic warfare capability. U.S. Army

[39] Army Techniques Publication 3-12.3, C-1.

BCTs have limited access to EW collection equipment and minimal manning while the Russian Army appears to have the capability to collect across all wavelengths within the electromagnetic spectrum.

Network Integration Exercise 17-2, held at Fort Bliss, Texas in July 2017 provided the U.S. Army with the opportunity to test new equipment and validate emerging technologies. It also provided the opportunity to employ U.S. systems in a contested environment against EW systems that are currently fielded by adversarial militaries around the world. The exercise, not specifically designed to stress U.S. capabilities, proved a massive gap in capability relative to likely enemies. Threat EW systems were able to gain near immediate situational understanding of U.S. positions, assets and scheme of maneuver while the U.S. ability to counter those actions or gain understanding of adversarial positions was negligible.[40] This exercise demonstrated the difference in current capability and identified a gap that requires immediate attention.

The exercise also showed the value in having electronic attack capability at the lowest tactical level, enabling maneuver commanders to provide specific effects on an adversary to support tactical maneuver. The threat EA systems were able to significantly disrupt friendly force operations and synchronization, at the time and place of choosing by the enemy commander. The U.S. Army does not possess a similar capability within BCTs nor does it have an active counter measure.

Chapter Summary

The U.S. Army is minimally manned, at the brigade level and below, with EW specialists and equipment. There is limited technological capability to conduct EW across

[40] After Action Review, US Army Network Integration Exercise 2017 at Fort Bliss, TX.

the breadth of a brigade area of operations and limited ability to conduct EW forward of the FLOT. Additionally, the U.S. Army does not have electronic attack capability within a BCT and relies on joint enablers that are neither reliable nor readily available. The lack of adequate manning and equipment puts U.S. forces at a marked disadvantage in land warfare relative to their adversaries.

The next chapter will look at electronic warfare technology and systems that currently exist within the U.S. Military and foreign armies. Those technologies will be studied to identify specific systems or concepts that can be fielded to fill the observed gaps within U.S. Army formations.

Electronic Warfare Technologies Currently Available

The U.S. Army, as described, is ill-prepared to counter adversarial electronic warfare capabilities and is not optimized to capitalize on threat EW signatures. Though much technology is under development within the Department of Defense, our allies and adversaries; a critical need exists for an immediate evolutionary solution while revolutionary changes are underway.[41] This immediate solution could come from allied or adversarial capability if properly researched and procured. The intent of this chapter is to explore EW collection, detection, and attack platforms and capabilities that currently exist and determine whether any would offer the U.S. a capability that exceeds current capacity and would offer the evolutionary change that is needed to remain viable in current conflict while new concepts of war and capabilities are developed for the next generation of conflict. Acknowledgement is made that procurement of new systems and capabilities is typically slow and purchasing military systems from foreign militaries is uncommon for the U.S. DoD.

Electronic Collection and Attack Assets Available

Collection of enemy signals helps to illuminate disposition, composition and strength of forces and aids commanders in understanding enemy actions. The U.S. Army has limited assets available to conduct this mission, though there are systems that exist that would help provide this capability to tactical formations. Gaining an understanding of the technology that currently exists, specifically the systems that other U.S. organizations,

[41] The author assesses that evolutionary development of EW capability is needed to modernize current equipment to ensure capability on the current battlefield, while also requiring revolutionary EW development that changes the way EW is conducted. Evolutionary change will modernize current systems while revolutionary change will develop entirely new concepts and capabilities.

allies and adversaries are employing on the battlefield will help inform analysis on systems that may be available to the U.S. Army to field in the short term.

The U.S. made AN/MLQ-36A, Mobile Electronic Warfare Support System (MEWSS), is currently fielded in limited quantities to United States Marine Corps Radio Battalions and has the capacity to detect and evaluate enemy communications, provide approximate locational information and disrupt adversarial communications on specified channels.[42] The equipment is mounted in a combat vehicle and provides battlefield situational awareness to commanders while enhancing the lethality of the formation by disrupting enemy communications and unmanned aerial systems. Though limited in range and capacity, the system provides the lowest echelon of leaders an EW capability. The system has the capacity to automatically transmit information to other systems and to a higher headquarters to allow for situational awareness across the battlefield and enhanced targeting capability.

The systems itself is mounted on a modified USMC Light Armored Vehicle, providing the operators protection while enabling them with mobility and sustainment. The system can be used while on the move but operates more effectively when stationary with the antennae mast extended to an elevation of up to 30 feet.[43]

The Russian made Krasuha-4 is a ground based, mobile EW platform that is designed to collect ground and aerial signals, adjudicate whether they are threat or friendly and determine the nature of the signals. This helps Russian forces discriminate incoming missiles and aircraft as well as ground radars and tactical signals at a range of up to 400

[42] Headquarters, United States Marine Corps, *Electronic Warfare*, Marine Corps Warfighting Publication 3-40.5 (Washington, DC: Department of the Navy, September 2002), 5-3.
[43] Headquarters, Department of the Army, *Electronic Warfare in Operations*, Field Manual 3-36 (Washington, DC: Department of the Army, February 2009), E-5.

km.[44] The Russian military typically uses this asset to support defense of critical systems, specifically long range precision fires assets and air defense systems, but it has the capability to detect and potentially disrupt or jam signals across the spectrum of communications. This capability allows Russian commanders the ability to determine threat activities, make decisions about kinetic or non-kinetic response to detected threats and conduct electronic attack as required to support the mission.

The Krasuha-4 is a vehicle mounted system, operating as a single vehicle or in concert with a towed shelter. The vehicle has 8 wheels, providing equal mobility to that of a medium logistics vehicle, and is equipped with a satellite dish and extendable mast that allows collection, transmission and communication over long ranges. The system is assessed to be able to be seamlessly integrate into tactical formations based on its mobility and speed.[45]

The U.S. made BAE Systems S-3000 family of signals intelligence equipment provides line of sight and beyond line of sight collection capability across the spectrum of communications signals and systems.[46] The systems can be mounted on vehicles or aerial systems and can facilitate enhanced understanding of battlefield operations for commanders at mid-level tactical echelons.[47] Though not currently fielded and still being developed and refined, the system has the potential to provide off-the-shelf capacity to

[44] Samuel Bendett, "America is Getting Outclassed by Russian Electronic Warfare," *The National Interest*, September 19, 2017, https://nationalinterest.org/feature/america-getting-outclassed-by-russian-electronic-warfare-22380 (accessed December 20, 2019).
[45] The precise characteristics or employment of the system are not entirely known. The assessment, by the author, is based on a compilation of understanding from readings and known pictures of the Krasuha-4.
[46] BAE Systems, *S-3000 Signals Intelligence & Information Operations Systems*, https://www.baesystems.com/en-us/product/s-3000-signals-intelligence-and-information-operations-systems (accessed January 27, 2020).
[47] Author assesses that mid-level tactical formations include Battalions and Brigade Combat Teams.

U.S. Army formations for collection and exploitation of enemy signals, including HF, VHF, UHF, satellite and GPS.

The Electronic Warfare Tactical Vehicle (EWTV) is under development and has been fielded for evaluation by some units in the U.S. Army. The vehicle provides an electronic collection and jamming capability to U.S. Army brigade combat teams.[48] The system has not been fielded beyond initial testing but shows a degree of optimism to support tactical commander's decision making and ability to leverage technology to gain a tactical advantage on an adversary. The EWTV, though still being refined, has the potential to be promulgated down to lower levels than the brigade combat team, once validated and determined to meet operational requirements.

The EWTV is mounted on a Mine Resistant Ambush Protected (MRAP) vehicle, providing tactical mobility and survivability to the crew. Aside from possessing multiple antennas, it looks like other MRAPs that are fielded across U.S. Army brigades and possesses an equal capability for mobility and survivability.[49]

The USMC operates the Communication Emitter Sensing and Attack System (CESAR) II within Radio Battalions that is specifically designed to jam adversarial communications across a majority of electronic networks and frequencies. It lacks the capability to exploit communications but can provide effective jamming of pre-

[48] John R. Hoehn, "Ground Electronic Warfare: Background and Issues for Congress," *Congressional research Service,* September 17, 2019, 9.
[49] Sydney J. Freeberg, "Army Test Jamming MRAPS: New Electronic Warfare Vehicle," *Breaking Defense,* August 16, 2018, https://breakingdefense.com/2018/08/army-tests-jamming-mraps-new-electronic-warfare-vehicle (accessed March 1, 2020).

determined threat communications networks and systems. The system is typically vehicular mounted but a variant exists that weighs 180 pounds and can be dismounted.[50]

The systems itself is not difficult to employ but it involves the transport of two antennas, base plates, radio systems and various cables and cords. It also requires batteries that must be carried and resupplied. The system, though not ideal for long range movements, provides enhanced forward EW presence and capability in a dismounted configuration.

The Russian made and employed Borisoglebsk-2 is an EW system that is designed to conduct passive electronic reconnaissance of adversarial communications and has the ability to jam and disrupt those communications across a significant frequency range.[51] Though unconfirmed, it has been reported that the system was used extensively is Eastern Ukraine by Russian forces in 2014 and 2015 as well as is Syria from 2015 through present. The system also has the capability to conduct reconnaissance and disruption of airborne communications and radar systems.[52]

The final system that Russia routinely employs is specifically designed to jam satellite signals, to include Global Positioning Systems (GPS) as well as long range digital communications. The Zhitel is a vehicle mounted system that has the ability to deny or spoof satellite signals and locations, as well as deny cellular phone use, across a 30 km area. The system has the capability to deny one hundred percent usage of frequencies within a particular range and all satellite signals within the designated range.[53] The

---

[50] Mathuel Browne, "Corps ready to wage electronic warfare with new mobile sensor, attack system," *Marines*, September 7, 2016, https://www.marcorsyscom.marines.mil/News/News-Article-Display/Article/936029/ (accessed December 20, 2019).
[51] Samuel Cranny-Evans, "Russia Trials new EW Tactics," *Janes*, June 14, 2019.
[52] Cranny-Evans.
[53] Army Recognition, "R-330ZH Zhitel jamming cellular satellite communication station technical data sheet pictures video" April 5, 2014 https://www.armyrecognition.com/russia_russian_missile_system_

system is often times employed in concert with the Borisoglebsk-2 and Krasuha-4 to collect and disrupt the entirety of the electronic spectrum.[54]

Chapter Summary

Electronic collection and attack capabilities are rapidly changing as electronic technology evolves at an unprecedented rate. The need for comprehensive EW change within the U.S. Army is evident and must include revolutionary changes in capabilities and techniques as we prepare for future conflicts. In the short term, adaptation of currently available evolutionary technology must be considered. The U.S. Army has begun to test systems that will add some limited capability, while the USMC has done the same. The Russian Army fielded systems that have the capability to collect and disrupt a vast majority of U.S. combat systems and capabilities on the current battlefield. Those capabilities and systems should be studied and used to support U.S. technological advancements in the short term to allow the U.S. to bridge the capabilities gap that currently exists while developing overmatch in future revolutionary EW systems.

The next chapter will identify specific systems and the requisite manning requirements that can be adopted immediately to facilitate evolutionary change in the EW capability of U.S. Army brigades.

vehicle_uk/r-330zh_zhitel_jamming_cellular_satellite_communication_station_technical_data_sheet_pictures_video.html (accessed January 27, 2020).

[54] Cranny-Evans.

Discussion and Recommendations

The U.S. Army is currently outmatched by peer adversaries in offensive and defensive electronic warfare (EW) capability. Russia demonstrated their EW capability in Ukraine and have shown significant equipment and synchronization capabilities in Syria. This military capability is used in accordance with their concept of New Generation Warfare, using influence to impact their adversary and EW to locate, disrupt and defeat their systems. The U.S. Army lacks the ability to effectively counter these threats. This deficiency could lead to unacceptable, but avoidable, levels of casualties suffered by U.S. ground combat formations if a change in equipping and manning is not made in the near term. While revolutionary change in EW equipment is necessary to surpass adversaries like Russia and China, an immediate, evolutionary change in equipment must be made to ensure U.S. dominance of ground conflict in the near term. There must be an acknowledgement that a deficiency exists and a willingness to use equipment currently in the U.S. military inventory, use technology that exists in adversarial systems and put wholehearted efforts into developing new technology to support the warfighter. These technological advancements must be accompanied by an increase in personnel manning to support use of the systems and enhance overall battlefield coverage and capacity for EW. Systems currently exist in the U.S. Military and within adversarial formations that can be immediately adopted to ensure equal capability in the event of conflict.

Equipping Recommendations

Infantry, armor and cavalry companies must be enabled with a capability to track enemy EW signature and use it to refine operations and prepare for contact. The Army should immediately field one Electronic Warfare Tactical Vehicle (EWTV), to each

maneuver company. This capability will give commanders the ability to observe, orient and disrupt adversarial communications from a singular vehicle mounted system. Additionally, companies should field two CESAR II dismounted EW systems that are man portable, enhancing the depth and breadth of the EW collection space for a company. These capabilities will allow company commanders to develop the enemy situation, answer Commander's Critical Information Requirements (CCIR) for the battalion or brigade commander and maximize kinetic and non-kinetic effects on the enemy.

Maneuver battalions must be enabled with the ability to detect, exploit and attack enemy electronic systems while protecting their own. They must also have the ability to analyze the signals that are collected from subordinate companies and rapidly determine the enemy scheme of maneuver or disposition should signals analysis. Battalions should field vehicle mounted BAE S-3000 EW systems, which will provide the Battalion Commander with the ability to collect and jam adversarial signals. This capability, coupled with the enhanced capability within each company will bring clarity on enemy disposition and scheme of maneuver and disrupt their ability to synchronize maneuver in the close fight.

Brigade combat teams (BCTs) must be able to analyze adversarial signals, disrupt their ability to synchronize operations, coordinate fire support and provide mission command. To conduct these types of operations, BCTs should field a systems with equal capability to the Russian Krasuha-4. This vehicular mounted system has the ability to disrupt aircraft, radars, long range and tactical communications, and GPS. This capability gives the BCT Commander the ability to shape the battlefield through disruptive EW and

precision fires, allowing battalions and companies to conduct offensive and defensive maneuver against a degraded enemy. Use of this system at the BCT level will help deny the advantages that currently exist in the EW spectrum and allow U.S. forces that ability to conduct decisive ground maneuver.

Manning Recommendations

Manning within each echelon of command must be enhanced to increase capacity to analyze adversarial EW actions as well as operate newly fielded EW systems.

In order to properly man the EWTV and CESAR II system at the company level, manning should be increased by a nine man squad; a staff sergeant and two soldiers to operate the EWTV and a sergeant and two soldiers for each of the CESAR II systems. This increase in manpower will allow the squad to operate each of the three systems independently while giving the squad leader the ability to synchronize EW actions across the company and coordinate EW battlespace with adjacent units. There will be limited ability to analyze all of the signals collected or disrupted but will facilitate communication with the battalion analysis cell.

Battalions need to be manned with personnel to support employment of the two S-3000 systems, each of which require a crew of three. Additionally, battalions should have a 4 man EW analysis team that works in the S3 or S2 sections. These soldiers will analyze the electronic signatures that are being collected by the company and battalion collection platforms and provide recommendations to the commander on kinetic and non-kinetic means to neutralize or exploit the threat. The vehicles should be manned by a sergeant and two soldiers while the exploitation team should be manned by a lieutenant (LT), a sergeant first class (SFC) and two soldiers. The LT and SFC will also serve as the

officer in charge (OIC) and non-commissioned officer in charge (NCOIC) of EW operations across the battalion.

Brigades should be manned with one team of five soldiers to operate the system that has equal capabilities to the Russian Krasuha-4. Additionally, they should be manned with a BCT level exploitation cell that includes eight soldiers, including a major (MAJ), master sergeant (MSG), two SFCs, and four soldiers. The MAJ and MSG will also serve as the OIC and NCOIC of EW operations across the brigade battlespace. This enhanced capability will facilitate the BDE Commander's operation of BDE level platforms while synthesizing the signals that have been collected across the battlespace to deliver necessary disruptive or destructive effects on the adversary.

Training Recommendations

In order to ensure soldiers across the formations are comfortable with the employment of enhanced EW capability while understanding the intricacies of synchronization of systems and communication between assets, training needs to be conducted at each echelon. From individual skills, at the company level, through collective exercises at the brigade level, all training should include electronic warfare.

In order to allow EW to become second nature to soldiers understanding of battlefield effects it must be integrated into every training event and exercise. Similar to medical, fire support and logistics operations being part of all training that is conducted at the squad level and higher, EW must be incorporated as well. Training for the EW teams within each company should include collection and dissemination of EW signature and intelligence as part of squad and platoon situational and live fire training exercises. Squad and platoon leaders must be comfortable maneuvering EW teams throughout the

battlefield, attaching and detaching the company level teams to their formations and requesting specific intelligence, refining EW objectives and refining maneuver based on EW collection and input.

A significant challenge to higher level collective training, at the battalion and brigade level, is having enough EW assets training together and gathering enough intelligence to stress the analytical capability of the staff and the decision making of the commanders to employ lethal and non-lethal effects based on EW collection. This training should be incorporated into the Combat Training Centers and the treat EW signature should be robust enough to require continuous collection, analysis and action by training formations. EW cannot be an afterthought or an event during a training exercise that is not continuous. Employment of EW against the enemy and protection from enemy EW attack and collection must be continuous in all collective training events.

Discussion

The electronic warfare threats posed by Russia are significant. In order to counter their capability, the U.S. Army needs to make immediate evolutionary changes to EW systems and personnel manning. Without immediate changes, the U.S. Army risks being defeated during modern armed conflict. The immediate evolution of EW capability must occur simultaneously to developing revolutionary systems and concepts that allow U.S. forces to establish overmatch against peer adversaries.

There is significant technology that still doesn't exist that will prove to be decisive on future battlefields. There is technology that exists in adversarial formations that is unknown by the U.S. and the capabilities are misunderstood or misinterpreted. This fact alone reinforces the need to make immediate and drastic changes to how the U.S. Army

is equipped for the next fight. The current organization is inadequate to counter the known threats and provides little ability for commanders to exploit enemy weaknesses or opportunities. It is currently designed as reactive and passive, and inadequate to counter peer adversaries. The equipment currently being used is antiquated in capability and inadequately distributed across formations. In order to address the immediate shortcoming in personnel, equipment and training, the U.S. Army should be manned and equipped in accordance with the recommendations in table 5.1.

	Equipping	**Manning**
Company (15 per BCT)	1 x EWTV	9 x EW System Operators
	2 x CESAR II	
Battalion (4 per BCT)	2 x S-3000	6 x EW System Operators
		4 x EW Analysts
Brigade Combat Team	Krasuha-4 (or similar)	5 x EW System Operators
		8 x EW Analysts
Total	15 x EWTV	164 x EW Systems Operators
	30 x CESAR II	24 x EW Analysts
	8 x S-3000	
	1 x Krasuha-4	188 x Total Personnel

Table 5.1: Recommended Equipping and Manning within U.S. Army Brigade Combat Teams

The recommendations are not all inclusive but present an immediate way to address an immediate deficiency in capability. The number of additional soldiers needed is the equivalent of a large company and is consistent with the scope of EW manning that is seen in adversarial formations. These 188 additional soldiers could come from the number of soldiers currently assigned to the units or could be added to the end strength of each brigade. Either way, there is an identified gap in ability and a feasible and acceptable way to address the gap with current capabilities.

Additional research should be conducted on emergent technologies that can enhance current technologies in the near term while analysis on adversarial systems must be continuous. Risk exists in countering current threats without taking into consideration emergent threats that will exist on the future battlefield. Research for this thesis did not include thorough analysis on emergent capabilities that peer adversaries will possess in the next ten to twenty years.

Chapter Summary

The U.S. is not equipped or manned to engage in active ground combat with peer adversaries. This is largely due to inadequate Electronic Warfare capability and manning. These issues must be immediately addressed with an evolutionary change in capacity while industry develops systems that will allow for revolutionary change and provide overmatch against peer adversaries. To meet the threat that currently exists, the U.S. Army should field systems that are currently available while increasing manning levels within each brigade combat team by 188 soldiers. This will address the immediate deficiency and allow U.S. Army forces the ability to compete with peer adversaries on the modern battlefield.

Conclusion

The United States has begun competition between revisionist and revanchist powers that has highlighted deficiencies in areas where the U.S. has historically enjoyed overmatch. Russia demonstrated a highly sophisticated EW architecture in Eastern Ukraine that synthesized tactical EW collection, disruption and targeting. They coupled that with kinetic fires that delivered complete destruction to Ukrainian formations and personnel. The U.S. is equally prepared to defeat those systems as the Ukrainians were in 2014 and without significant, immediate changes to equipment and personnel, the U.S. risks suffering a similar result if engaged in active ground combat with the Russian military or an adversary equipped with Russian technology.

In order to make an immediate change to U.S. Army capability, systems that currently exist should be fielded to brigade combat teams and personnel should be added to man those systems and provide the requisite analysis of the signals collected. While fielding available systems and inducing an evolutionary upgrade to capability, the U.S. Army should engage industry to develop the next generation of EW capability to facilitate a revolutionary upgrade to ground electronic warfare and reestablish American dominance on the battlefield.

Without evolutionary and revolutionary change, the U.S. risks suffering decisive defeat on a modern or future battlefield against a peer adversary.

Bibliography

After Action Reviews, Joint Readiness Training Center.

After Action Review, US Army Network Integration Exercise 2017 at Fort Bliss, TX.

After Action Review, Cyber Quest 2018 and Cyber Center of Excellence / Cyber Battle Lab discussions.

Army Recognition. *R-330ZH Zhitel jamming cellular satellite communication station technical data sheet pictures video*. April 5, 2014. https://www.armyrecognition.com/russia_russian_missile_system_vehicle_uk/r-330zh_zhitel_jamming_cellular_satellite_communication_station_technical_data_sheet_pictures_video.html (accessed January 27, 2020).

Asymmetric Warfare Group. *Russian New Generation Warfare Handbook, Version 1*. Washington DC: Asymmetric Warfare Group, December 2016.

BAE Systems. *S-3000 Signals Intelligence & Information Operations Systems.* https://www.baesystems.com/en-us/product/s-3000-signals-intelligence-and-information-operations-systems (accessed January 27, 2020).

Bendett, Samuel. "America is Getting Outclassed by Russian Electronic Warfare." *The National Interest.* September 19, 2017.https://nationalinterest.org/feature/america-getting-outclassed-by-russian-electronic-warfare-22380 (accessed December 20, 2019).

Boyd, Andrew. "Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army." *The Institute of Land Warfare*, November 2017.

Brown, Daniel. "Russian-backed separatists are using terrifying text messages to shock adversaries — and it's changing the face of warfare." *Business Insider.* August 14, 2018.

Browne, Mathuel. "Corps ready to wage electronic warfare with new mobile sensor, attack system." *Marines.* September 7, 2016. https://www.marcorsyscom.marines.mil/News/News-Article-Display/Article/936029/ (accessed December 20, 2019).

Collins, Liam. "Russia Gives Lessons in Electronic Warfare." *Association of the United States Army.* July 26, 2018. https://www.ausa.org/articles/russia-gives-lessons-electronic-warfare (accessed November 10, 2019).

Cranny-Evans, Samuel. "Russia Trials new EW Tactics." *Janes*. June 14, 2019.

Freeberg, Sydney J. "Army Test Jamming MRAPS: New Electronic Warfare Vehicle." *Breaking Defense.* https://breakingdefense.com/2018/08/army-tests-jamming-mraps-new-electronic-warfare-vehicle/ (accessed March 1, 2020).

Freedberg, Sydney J. "HASC EW Expert Bacon: US 'Not Prepared' for Electronic Warfare vs. Russia, China." *Breaking Defense*. https://breakingdefense.com/2018/01/hasc-ew-expert-bacon-us-not-prepared-for-electronic-warfare-vs-russia-china/ (accessed September 23, 2019).

Grau, Lester and Bartles, Charles. *The Russian Way of War.* Fort Leavenworth: Foreign Military Studies Office, 2016.

Headquarters, Department of the Army. *Cyberspace and Electronic Warfare Operations.* Field Manual 3-12. Washington DC: Department of the Army, April 2017.

Headquarters, Department of the Army. *Electronic Warfare in Operations*. Field Manual 3-36. Washington DC: Department of the Army, February 2009.

Headquarters, Department of the Army. *Brigade Combat Team.* Field Manual 3-96. Washington DC: Department of the Army, October 2015.

Headquarters, Department of the Army. *Electronic Warfare Techniques*. Army Techniques Publication 3-12.3. Washington DC: US Government Printing Office, 2019.

Headquarters, United States Army Special Operations Command. *Little Green Men: a Primer on Modern Russian Unconventional Warfare, Ukraine 2013-2014*. Fort Bragg, NC: United States Army Special Operations Command, 2016.

Headquarters, United States Marine Corps. *Electronic Warfare*. Marine Corps Warfighting Publication 3-40.5. Washington DC: Department of the Navy, 2002.

Hoehn, John R. "Ground Electronic Warfare: Background and Issues for Congress." *Congressional research Service*. September 17, 2019.

Interview with current Military Intelligence Company Commander within a Brigade Combat Team.

Jones-Bonbrest, Nancy. "Electronic Warfare Prototypes Improve Operational Understanding Against Near-Peer Threats." *Army Rapid Capabilities and Critical Technologies Office*. May 10, 2018. http://rapidcapabilitiesoffice.army.mil/news/Electronic-warfare-prototypes-improve-operational-understanding/ (accessed September 19, 2019).

Karber, Phillip. “Russia’s New Generation Warfare.” *Association of the United States Army,* May 20, 2016.

Kjellen, Jonas. “Russian Electronic Warfare: The Role of Electronic Warfare in the Russian Armed Forces,” *FOI,* September 2018.

McDermott, Roger N. “Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum.” *International Centre for Defense and Security* September 2017.

Multi-National Training Group-Ukraine, Bi-annual Report.

Spring-Glace, Morgan J. “Return of Ground-Based Electronic Warfare Platforms and Force Structure.” *Military Review,* July-August 2019.

Stowell, Joshua. “What is Hybrid Warfare?” *Global Security Review,* August 1, 2018.

U.S. Army Directorate of Force Management. *Force Management System Website*. https://fmsweb.fms.army.mil/unprotected/splash/ (accessed September 23, 2019).

U.S. Congressional House Committee on the Armed Services. *Hearing on Readying the U.S. Military for Future Warfare, 115th Congress, 2nd session, January 30, 2018*. Washington DC: Government Printing Office. 2018.

U.S. Joint Chiefs of Staff. *Cyberspace Operations.* Joint Publication 3-12. Washington DC: Joint Chiefs of Staff, June 8, 2018.

U.S. Senate Subcommittee on Emerging Threats and Capabilities on the Armed Services. *Russian Influence and Unconventional Warfare Operations in the Gray Zone: Lessons from Ukraine*. Washington DC: CreateSpace Independent Publishing Platform. 2018.

Varfolmeeva, Anna. “Signaling strength: Russia’s real Syria success is electronic warfare against the US.” *The Defense Post*. May 1, 2018. https://thedefensepost.com/2018/05/01/russia-syria-electronic-warfare/ (accessed 16 SEP 2019).

Wong, Doni, Lipsky, Theodore, Calhoun, Briged and Cruz, Pablo. “Integration of Signals Intelligence, Electronic Warfare in Reconnaissance Troop: Seeing Where the Eye Cannot See.” *Armor Magazine* (Fall 2018): 13-19.