

Satellite and Ground Communication Systems:
Space and Electronic Warfare Threats
to the
United States Army

A Monograph

by

MAJ Andrew H. Boyd
US Army



School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

2017

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) 01-02-2017		2. REPORT TYPE SAMS Monograph		3. DATES COVERED (From - To) JUN 2016 – MAY 2017	
4. TITLE AND SUBTITLE Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Major Andrew H. Boyd				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) School of Advanced Military Studies (SAMS) 201 Reynolds Avenue Fort Leavenworth, KS 66027-2134				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) Command and General Staff College 731 McClellan Avenue Fort Leavenworth, KS 66027-1350				10. SPONSOR/MONITOR'S ACRONYM(S) CGSC	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT Approved for Public Release; Distribution Unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT Threats to communication satellites and ground communication systems will present significant challenges to the US Army in a conventional war. The US Army is significantly dependent on satellite communication for the planning and execution of operations. In an austere environment, most of the Army's high-data mission command systems cannot function without satellite connectivity. Potential belligerents' counter-space capabilities can disrupt the Army's access to satellite communication, and US forces operating at northern extremes may not have connection due to geosynchronous satellite geometry. This would leave US forces more reliant on their terrestrial communication systems. Although the US Army has a strong historical precedent for countering electronic warfare threats to its ground communication systems, disciplined electronic protection has deteriorated since the end of the Cold War due to waning threats and to an apparent technological superiority. This leaves the Army with little capability to counter the increasing electronic warfare capability that would target US communication systems. Given the threats to satellite and ground communication systems, the US Army is unlikely to be successful in a conventional war against a comparable adversary without significant change to equipment, doctrine, and training.					
15. SUBJECT TERMS Counter-space; satellite communication; electronic warfare; jamming; direction finding; geosynchronous satellite geometry; China; Russia.					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES 49	19a. NAME OF RESPONSIBLE PERSON Major Andrew H. Boyd
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified			19b. TELEPHONE NUMBER (include area code) 913-758-3302

Monograph Approval Page

Name of Candidate: Andrew H. Boyd

Monograph Title: Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army

Approved by:

_____, Monograph Director
Melissa A. Thomas, PhD

_____, Seminar Leader
Joseph A. Schafer, COL

_____, Director, School of Advanced Military Studies
James C. Markert, COL

Accepted this 25th day of May 2017 by:

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

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

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

Abstract

Satellite and Ground Communication Systems: Space and Electronic Warfare Threats to the United States Army, by MAJ Andrew H. Boyd, USA, forty-nine pages.

Threats to communication satellites and ground communication systems will present significant challenges to the US Army in a conventional war. The US Army is significantly dependent on satellite communication for the planning and execution of operations. In an austere environment, most of the Army's high-data mission command systems cannot function without satellite connectivity. Potential belligerents' counter-space capabilities can disrupt the Army's access to satellite communication, and US forces operating at northern extremes may not have connection due to geosynchronous satellite geometry. This would leave US forces more reliant on their terrestrial communication systems. Although the US Army has a strong historical precedent for countering electronic warfare threats to its ground communication systems, disciplined electronic protection has deteriorated since the end of the Cold War due to waning threats and to an apparent technological superiority. This leaves the Army with little capability to counter the increasing electronic warfare capability that would target US communication systems. Given the threats to satellite and ground communication systems, the US Army is unlikely to be successful in a conventional war against a comparable adversary without significant change to equipment, doctrine, and training.

Contents

Acknowledgement	v
Acronyms.....	vi
Illustrations	ix
Introduction	1
Satellite Communication: US Army's Dependence	3
Satellite Communication: Limitations and Vulnerabilities.....	7
SATCOM Limitations	7
SATCOM Vulnerabilities	12
Lack of SATCOM Redundancy	19
Terrestrial Communication: Increased Need and Renewed Threat	22
A Precedent for Emission Control	22
Apathy towards a Renewed EW Threat.....	30
Recommendations	39
Equipment.....	39
Doctrine	42
Training.....	43
Conclusion.....	44
Bibliography	45

Acknowledgement

I would like to thank my advisor, Dr. Melissa Thomas, for the support and encouragement during my research and writing of this monograph. I would also like to thank my wife, Amanda, for being a thorough editor and coach.

Acronyms

AEF	American Expeditionary Force
AEHF	Advanced Extremely High Frequency
AFATDS	Advanced Field Artillery Tactical Data System
AFRICOM	Africa Command
AOA	Angle of arrival
ASAT	Anti-satellite missile
ATP	Army Techniques Publication
BFT	Blue Force Tracking
CEP	Circular error probable
CME	Coronal Mass Ejection
CNR	Combat Net Radio
CPOF	Command Post of the Future
CTC	Combat training center
D/F	Direction finder
DCGS	Distributed Common Ground System
DIA	Defense Intelligence Agency
DOA	Direction of arrival
DoD	Department of Defense
DOT&E	Director, Operational Test and Evaluation
ECCM	Electronic counter-countermeasures
ECM	Electronic countermeasures
EPS	Enhanced Polar System
EPLRS	Enhanced Positioning Locating and Reporting System
EW	Electronic warfare
FBCB2	Force XXI Battle Command Brigade and Below
FOT&E	Follow-on Operational Test and Evaluation

FM	Field Manual
FMI	Field Manual Interim
Gbps	Gigabits per second
GEO	Geosynchronous earth orbit
GPS	Global Positioning System
HF	High frequency
HNW	High-band Networking Waveform
ICE	Interference Cancellation Equipment
ISB	Intelligence Science Board
JBC-P	Joint Battle Command-Platform
Kbps	Kilobits per second
Km	Kilometer
LAN	Local Area Network
LEO	Low-earth orbit
Mbps	Megabits per second
MCPN	Marine Corps Prepositioning Program-Norway
MNVR	Mid-Tier Networking Vehicular Radio
MUOS	Mobile User Objective System
NATO	North Atlantic Treaty Organization
OSCE	Organization for Security Cooperation in Europe
PLA	People's Liberation Army
SATCOM	Satellite communication
SINCGARS	Single Channel Ground Airborne Radio System
SNAP	Steerable Null Antenna Processor
SSL	Single-site location
UAV	Unmanned aerial vehicle
UHF	Ultra-high frequency

USCC	US-China Economic and Security Review Commission
VHF	Very-high frequency
WGS	Wideband Global SATCOM
WIN-T	Warfighter Information Network-Tactical

Illustrations

1	Terrain effects on SATCOM.	9
2	Trondheim, Norway.....	10
3	Satellite orbits, periods and footprints.	15
4	Notional direction finding of division command posts in Azerbaijan.	23
5	Notional single-site location (SSL) in Azerbaijan.	24
6	Plessey Interference Cancellation System.	28
7	R-330B direction finder.	34
8	R-378AM direction finder and jammer.	34
9	Relative capacity improvement of directional antennas.	39
10	Possible directional antennas for combat net radio.....	40
11	Comparison of omnidirectional antennas with directional antennas.	40

Introduction

The Athenians are addicted to innovation, and their designs are characterized by swiftness alike in conception and execution; you have a genius for keeping what you have got, accompanied by a total want of invention, and when forced to act you never go far enough.

It is the law, as in the arts so in politics, that improvements ever prevail; and though fixed usages may be best for undisturbed communities, constant necessities of action must be accompanied by the constant improvement of methods. Thus it happens that the vast experience of Athens has carried her further than you on the path of innovation.

—Thucydides, *History of the Peloponnesian War*

United States ground forces are significantly vulnerable in future conflict due to a dangerous reliance on satellite communication (SATCOM) and a lack of readiness to fight in the face of a growing counter-space and communications electronic warfare (EW) threat. Although SATCOM provides significant advantages over terrestrial communication systems, it carries some liabilities for which the US Army is ill-prepared. Coinciding with the Army's dependence on SATCOM, there is a lethargic institutional response to the unyielding proliferation of EW threats facing terrestrial communications. Although the US military's overall technological lead over near-peer threats has narrowed, the US Army continues to train and equip as though there is little technological threat to its communication practices and as if SATCOM is guaranteed. This complacency is accompanied by the procurement of high-data communication and mission command systems that deny ground forces both the flexibility and electronic protection they need to communicate and fight effectively in an environment where both space and the electromagnetic spectrum are contested.

One of the US Army's most critical vulnerabilities is its overreliance on SATCOM, on which most of its mission command systems depend. Most of the Army's mission command systems have developed to require data rates so high that the only way for them to function in an expeditionary role is through SATCOM. The increasing need for SATCOM bandwidth has led the US military to channel its operational communications through the leased networks of commercial

satellites, which lack adequate protection against jamming and are susceptible to state-actor influence.

Potential adversaries of the United States, such as the Russian Federation and the People's Republic of China, have long recognized US dependence on SATCOM and have developed formidable capabilities—such as jamming and anti-satellite missiles—to attack that dependence. Even without human threats to SATCOM, periodic geomagnetic storms have the potential to damage all satellites in orbit. Besides these challenges, most communication satellites do not function north of 65°N latitude, which includes zones for potential conflict with Russia. Despite these concerns, most ground force communications are structured to require consistent SATCOM.

As the US Army's celestial communication systems have enjoyed an apparent sanctuary in space, terrestrial communications EW has been put on the back burner. Advances in US electronic counter-countermeasures (ECCM), the fall of the Soviet Union, and the low EW threat in the conflicts in Iraq and Afghanistan are factors that have contributed to the Army's apathy toward communications protection. Current doctrinal manuals that cover communication practices and electronic warfare often lack the depth and tactical solutions that Cold War doctrine once provided to combat the EW threat. As well, the decision to field ground communication systems with highly detectable electromagnetic signatures is very reflective of an Army doctrine and culture that does not appreciate the potential of a terrestrial communications EW threat.

To overcome these significant vulnerabilities, the US Army must procure communications systems that maintain the information high ground, but also allow redundancy, flexibility, and survivability against threat counter-space and EW capabilities. As well, the Army must refine its doctrine to place proper emphasis on the threat of electronic attack and detection. Individual and collective training should combine the right equipment and techniques to ensure units are training for a realistic fight, which would include periods of denied SATCOM and increased threat of electronic attack and reconnaissance.

Upon assuming duties as the Chief of Staff of the Army, General Mark A. Milley said, “If we do not maintain our commitment to remain strong in the air, on the sea and yes, on the ground, then we will pay the butcher’s bill in blood, and we will forever lose the precious gift of our freedom.”¹ A key element of remaining strong on the ground is maintaining the capability to effectively communicate on the ground. If the Army loses SATCOM or faces a sophisticated terrestrial EW threat in conflict, it will still continue its mission and fight. The Army’s leaders and soldiers will surely adapt to any future conflict, regardless of how well the first battle goes. However, the equipment, training, and doctrine of today will determine how steep that learning curve is and what price in blood the US Army will pay. Currently, the Army’s communication vulnerabilities will face increasingly eager and sophisticated threats, and the benefit of prescient groundwork in peace is preferable to costly improvisation in a time of war.

Satellite Communication: US Army’s Dependence

Satellite Communication (SATCOM) is a critical component of tactical ground force communication structure. SATCOM allows command posts to communicate over great distances and at high data rates that terrestrial radio systems cannot achieve. The Single Channel Ground Airborne Radio System (SINCGARS) provides voice communication only up to 40 kilometers (km), and provides no more than 16 kilobits per second (Kbps) of data.² High Frequency (HF) radios can transmit voice and data over thousands of kilometers through ionospheric refraction (by bouncing off the ionosphere), but data rates are limited to 9.6 Kbps,³ which is insufficient for most

¹ Dan Lamothe, “‘We Will Pay the Butcher’s Bill in Blood’: General Issues Stern Warning as He Becomes Army Chief,” *Washington Post*, August 14, 2015, <https://www.washingtonpost.com/news/checkpoint/wp/2015/08/14/we-will-pay-the-butchers-bill-in-blood-general-issues-stern-warning-as-he-becomes-army-chief-of-staff/>.

² Field Manual (FM) 6-02.72, *Tactical Radios* (Washington, DC: Government Printing Office, 2002), I-2.

³ Field Manual (FM) 3-55.93, *Long-Range Surveillance Unit Operations* (Washington, DC: Government Printing Office, 2009), 6-18.

mission command systems. As well, volatile ionospheric conditions can significantly degrade the quality of HF transmission. The ground-based Enhanced Positioning Locating and Reporting System (EPLRS) limits users to 57.6 Kbps, with a brigade user community constrained to an area roughly 47 x 47 km.⁴ Military communication satellites—operating high above the earth and at higher frequencies—are often better suited to communicate across much longer distances and with higher data rates than most terrestrial systems.

SATCOM has considerable advantages over terrestrial systems in operational reach, data, and stealth. Because the majority of military communication satellites orbit 35,790 km above the earth's surface in a geosynchronous manner,⁵ line-of-sight issues are normally not a problem for separated ground elements attempting to employ their capabilities over great distances. For operations in Iraq and Afghanistan—still ongoing at the time of this writing—both countries' proximity to the equator allows SATCOM to function without terrain or man-made structures frequently blocking connection between the ground terminal and the satellite. As well, SATCOM provides data rates much higher than lower-frequency, terrestrial systems discussed above. The Advanced Extremely High Frequency (AEHF) joint-service satellite system can provide up to 8 megabits per second (Mbps) for as many as 6,000 terminals between the 65°N and 65°S latitudes.⁶ SATCOM ground terminals are also more immune to terrestrial EW attack and interception than most combat net radio (CNR). Because ground terminals connect with communication satellites by pointing directional antennas up into space, they avoid the effects of terrestrial threat jammers and deny a horizontal signal to enemy direction finders. Because the friendly electromagnetic signature

⁴ Michael R. Frater and M. J. Ryan, *Electronic Warfare for the Digitized Battlefield*, The Artech House Information Warfare Library (Boston: Artech House, 2001), 48.

⁵ Richard S. Deakin, *Battlespace Technologies: Network-Enabled Information Dominance* (Boston, MA: Artech House, 2010), 317.

⁶ Bert Chapman, *Space Warfare and Defense: A Historical Encyclopedia and Research Guide* (Santa Barbara, CA: ABC-CLIO, 2008), 139.

is not being transmitted horizontally over the earth—as is the case with terrestrial, line-of-sight radio—enemy sensors have difficulty detecting the vertical “uplink” transmissions going from earth to space.

As SATCOM has provided the warfighter with increased operational reach, data, and stealth, the US Army has increased its dependence on SATCOM. During the Gulf War, up to sixty satellites supported the transfer of operational data, allowing US ground units beyond the range of CNR to keep pace with rapid developments on the battlefield.⁷ The throughput of digital information during the Gulf War “gave the war a new dimension”⁸ and paved the way for the further proliferation of military SATCOM; dependence on bandwidth increased thirtyfold in the thirteen years between Operation Desert Storm and Operation Iraqi Freedom.⁹ Over the past fifteen years, SATCOM-enabled Blue Force Tracking (BFT) slowly eclipsed the terrestrial EPLRS as the primary communication medium for Force XXI Battle Command Brigade and Below (FBCB2). By 2017, the US Army will completely divest EPLRS.^{10,11} A 2004 RAND study argues that terrestrial line-of-sight radio will not be sufficient to meet US Army data needs, and that SATCOM will continue to become even more crucial for Army operations.¹² An Intelligence Science Board (ISB) report predicts that by 2020, total demand for SATCOM bandwidth will increase from 40 gigabits

⁷ Christopher H. Sterling, ed., *Military Communications: From Ancient Times to the 21st Century* (Santa Barbara, CA: ABC-CLIO, 2008), 300.

⁸ Ibid, 202.

⁹ Edward Byrne and Paul Konyha, eds., *Space Primer* (Maxwell Air Force Base, AL: Air University Press, 2009).

¹⁰ Blue Force Tracking (BFT) communicates GPS-enabled position location information (PLI) and text via commercial L-Band SATCOM, while EPLRS communicates such information through line-of-sight terrestrial UHF radio and automatic mobile relay.

¹¹ Patrick J. Donahue and United States Army Forces Command, “Force Command Mission Command Network Priorities,” April 26, 2016, 1–3.

¹² Joe Leland and Isaac Porche, *Future Army Bandwidth Needs and Capabilities* (Santa Monica, CA: RAND, 2004), 42.

per second (Gbps) today to 80 Gbps by 2022; projected SATCOM coverage will only be capable of providing up to 50 Gbps.¹³

Mission command systems such as the Distributed Common Ground System (DCGS), Command Post of the Future (CPOF), and Advanced Field Artillery Tactical Data System (AFATDS) typically rely on a SATCOM-enabled local-area network (LAN) for communication. DCGS, an intelligence-sharing product, requires a large amount of bandwidth,¹⁴ meaning the only way that DCGS *can* function—in an immature theater—is through a SATCOM-enabled LAN. CPOF can function at rates as low as 5 Mbps for about 300 users,¹⁵ but this rate is beyond the capabilities of the terrestrial radio systems (SINCGARS, HF, EPLRS) discussed above. Although the Advanced Field Artillery Tactical Data System (AFATDS) has the redundancy to communicate via LAN, terrestrial radio, and field wire, few mission command systems have this flexibility. Without system modification, DCGS, CPOF, and other mission command systems will only function with SATCOM in an expeditionary environment. In an immature theater without advanced infrastructure such as fiber optic cable, many of the Army’s mission command systems that support warfighting will not function if satellite connectivity is lost.

¹³ Intelligence Science Board, “Integrated Sensor-Collected Intelligence” (Washington, DC: Department of Defense, 2008), 25.

¹⁴ Kevin McCaney, “Army Still Catching Flak for Tactical Intell System,” *Defense Systems*, March 22, 2016, <https://defensesystems.com/articles/2016/03/22/army-dcgs-a-criticism.aspx>.

¹⁵ Harry Greene et al., “Command Post of the Future: Successful Transition of a Science and Technology Initiative to a Program of Record,” *Defense Acquisition Research Journal* 17 no. 1, no. 53 (January 2010): 11.

Satellite Communication: Limitations and Vulnerabilities

The logic of war usually leads belligerents to fight with whatever tools are at hand.

—Gideon Rose, *How Wars End*

Spaced-based satellite relay is the obvious choice for providing long-range reliable communications...However the vulnerability of satellites in the future suggests that it would be unwise to rely exclusively on such systems.

—Timothy Garden, *The Technology Trap*

SATCOM Limitations

Dependence on SATCOM comes with an array of geographic limitations and terrain interference. Most significant is the geographic limitation of the satellite “footprints” to between 65°N and 65°S, which define the areas in which ground terminals can connect to a satellite and vice versa.¹⁶ Some may not consider this a significant concern for US ground forces, since the threat of armed conflict does not seem to be developing at these northern and southern extremes. However, recent tension between the North Atlantic Treaty Organization (NATO) and Russia make conflict on the Scandinavian Peninsula plausible. US forces should be prepared to fight beyond 65°N in this region, but SATCOM will not be a dependable form of communication.

Half of Norway lies north of 65°N latitude, and this key NATO ally shares a 120-mile border with Russia, which has shown itself to be a reemerging threat since its 2008 invasion of Georgia. While some may consider NATO and the other Nordic countries currently safe from Russian invasion, a 2015 Russian training exercise that rehearsed a contingency invasion of Norway, Finland, Denmark, and Sweden shows otherwise. In the exercise scenario, Russia simulated the invasion of these states in order to control access to the Baltic Sea, denying NATO

¹⁶ Byrne and Konyha, *Space Primer*, 188..

the ability to reinforce its allies in Eastern Europe.¹⁷ In response to a 2016 deployment of 330 US Marines to a Norwegian airfield, a Russian defense official warned that Norway would now be on Russia's nuclear target list.¹⁸ Norway takes the threat of Russian aggression seriously enough that it has fielded a new unit to patrol the border with Russia. This outfit is more than a simple border and customs enforcement unit. It is armed with anti-armor and anti-aircraft capabilities, which serve to deter and disrupt a possible Russian ground invasion.¹⁹

As part of a plan to ensure that NATO members can defeat territorial incursions, the United States Marine Corps maintains significant prepositioned materiel in Norway. The Marine Corps Prepositioning Program-Norway (MCPN) owns a fleet of combat and support vehicles inside man-made caves to facilitate the equipping of a Marine expeditionary brigade for operations in support of NATO allies.²⁰ Given NATO's preparation and Russia's rhetoric, conflict in northern Europe is plausible. In such a conflict, US forces could easily find themselves fighting and communicating north of 65°N.

Not only do SATCOM footprints not extend beyond 65°N and 65°S, but the degree to which mountains, hills, and valleys affect satellite communication increases as ground communication terminals move further from the equator. Because most military communication

¹⁷ David Blair, "Russian Forces 'Practised Invasion of Norway, Finland, Denmark and Sweden,'" June 26, 2015, accessed on November 12, 2016, <http://www.telegraph.co.uk/news/worldnews/europe/russia/11702328/Russian-forces-practised-invasion-of-Norway-Finland-Denmark-and-Sweden.html>.

¹⁸ Matt Payton, "Norway Is Now a Nuclear Target," *The Independent*, November 1, 2016, <http://www.independent.co.uk/news/world/europe/norway-nuclear-target-us-marines-russia-politician-weapons-a7390386.html>.

¹⁹ Thomas Nilson, "Norway Creates New Army Unit on Border to Russia," *The Independent Barents Observer*, July 17, 2016, <http://thebarentsobserver.com/security/2016/06/norway-creates-new-army-unit-border-russia>.

²⁰ Tatum Vayavananda, "Marine Corps Equipment Rolls out of Classified Norwegian Caves," *United States Marine Corps*, December 2, 2016, accessed November 9, 2016, <http://www.marines.mil/News/News-Display/Article/655368/marine-corps-equipment-rolls-out-of-classified-norwegian-caves/>.

satellites orbit above the equator, these satellites will appear in the southern sky when observed from the Northern Hemisphere. As the observer in the Northern Hemisphere moves further north, the communication satellite will appear lower in the sky. In relatively flat, open terrain, this is not an issue as long as the ground terminal can ‘see’ and communicate with the communication satellite. However, if a ground terminal has elevated terrain or infrastructure to its south, it may not be able to communicate with the desired satellite. Any command and control systems that can *only* communicate through satellite-based communications will be nearly useless. As long as BFT, CPOF, and DCGS require SATCOM to function, those systems will be of no use to US ground forces operating in mountainous terrain near these northern extremes.

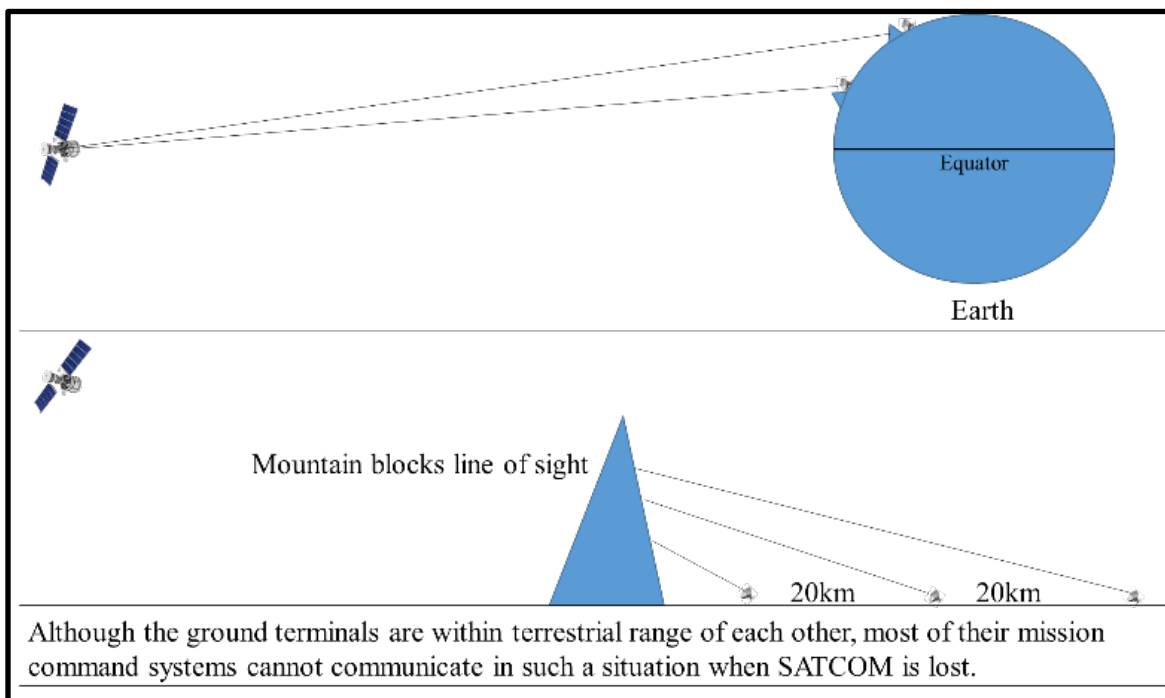


Figure 1. Terrain effects on SATCOM. Created by the author.

A useful illustration of this problem can be gleaned from the website, dishpointer.com. The website allows users to determine the azimuth and elevation to which they must orient their ground terminals in order to successfully connect to a satellite. Although the longitudes of most military communication satellites are not available at the time of this writing, the Eutelsat 12 commercial satellite will show line-of-sight challenges that are comparable to military SATCOM.

If US ground forces were to operate alongside NATO forces to deter or defeat Russian aggression on the Scandinavian Peninsula, military SATCOM would meet some significant challenges due to satellite geometry, man-made structures, and terrain. For example, some of the MCPP-N equipment is in a cave complex in Trondheim, Norway, which sits at 63.4305° latitude. This is technically within most SATCOM footprints, but subject to significant terrain interference. After expanding the port basing area, follow-on ground forces would likely have to deploy through Trondheim's port and fight across the peninsula around that same latitude. According to dishpointer.com, a SATCOM ground terminal in Trondheim must aim at 16° elevation to connect with a communication satellite similar to the Eutelsat 12 (Figure 2). At this latitude, even an object fifty meters away and only fifteen meters high would obstruct the satellite signal.²¹ In and around Trondheim, a dwelling just a few stories high could prevent successful communication.

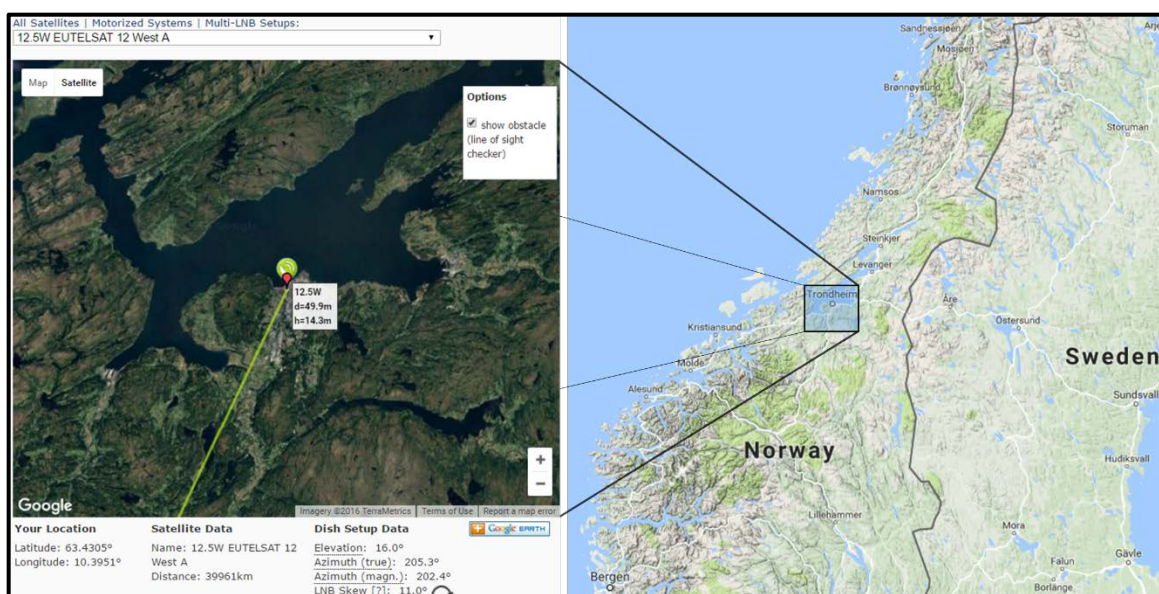


Figure 2. Trondheim, Norway and the required azimuth and elevation in order to achieve connectivity with the Eutelsat 12.

DishPointer, "Satellite Finder/Dish Alignment Calculator with Google Maps," accessed on November 8, 2016, <http://www.dishpointer.com>.

"Trondheim, Norway," Google Maps, accessed November 30, 2016, <https://www.google.com/maps/>

²¹ DishPointer, "Satellite Finder/Dish Alignment Calculator with Google Maps," accessed on November 8, 2016, <http://www.dishpointer.com>.

As movement and fighting through Norway would continue, the steep terrain lining many of Norway's main roads would likely prevent reliable SATCOM. Using the height-distance ratio above (15m: 50m), a hill or ridge only 60 meters in height and 300 meters away could prevent ground terminals from sending and receiving the data required for a common operational picture and friendly location reporting. As maneuver units approach latitudes closer to 65°N, the situation will force SATCOM terminals to lie exposed in open terrain in order to allow mission command systems to function. In the environment described above, the limited access to SATCOM would inhibit the ability of units to maneuver in the most advantageous terrain, forcing headquarters to expose themselves in open fields without any cover from hills or buildings and lacking concealment from vegetation. At this higher latitude and correspondingly lower aiming elevation, hilly terrain and man-made structures will cause decisions of maneuver to be subordinate to communication limitations. For US forces conducting potential operations at such northern extremes, SATCOM is more of a liability than an enabler. This raises questions about the ability of the US Army to fight a conventional ground war successfully when nearly all mission command systems are completely dependent on SATCOM.

Notwithstanding the limits of geosynchronous communication satellites, there are some military SATCOM constellations that can communicate with terminals beyond 65°N. Lockheed Martin claims that their Mobile User Objective System (MUOS) achieved successful Ultra High Frequency (UHF) voice and data connection on board an L-100 aircraft at 89.5°N. However, this connection was on an aircraft—therefore allowing an elevated line-of-sight advantage that ground units do not have—and the connection was only successful during “peak orbital conditions” of the supporting MUOS satellite.²² As well, the most recent testing of MUOS identified “200 high-

²² Lockheed Martin, “Lockheed Martin MUOS Satellite Tests Show Extensive Reach in Polar Communications Capability,” January 31, 2014, <http://www.lockheedmartin.com/us/news/press-releases/2014/january/131-ss-muos.html>.

priority hardware and software problems.”²³ Another system that can potentially function beyond 65°N is the up-and-coming Enhanced Polar System (EPS), which will consist of two satellites in opposing, highly-elliptical Molniya orbits.²⁴ This constellation will allow the two satellites to alternate in providing up to 18 Mbps of bandwidth between 65°N and 90°N to air, ground, and naval forces. Unfortunately, the EPS constellation is not yet in orbit to support operations; when it is in orbit, there will only be one satellite at a time to support all the potential SATCOM requirements—air, land, and maritime—north of 65°N.²⁵

SATCOM Vulnerabilities

Besides the geographic limitations of SATCOM, satellites are significantly vulnerable to some rare naturally-occurring events and emerging threat capabilities. Coronal mass ejections (CMEs) resulting in geomagnetic storms have the potential to cause significant damage to satellite electronics.²⁶ Potential adversaries such as Russia and China have attained the capability to exploit US space dependence through jamming and anti-satellite (ASAT) missiles. The hazard of threat capabilities is exacerbated by the US military’s preponderant use of commercial communication satellites, which are more vulnerable to jamming and cyber interference than military satellites. Even if US forces are operating in the optimal geographic area for successful satellite connectivity,

²³ Director, Operational Test and Evaluation, “FY 2015 Annual Report,” January 2016, 260.

²⁴ Department of Defense, “Enhanced Polar System (EPS),” Selected Acquisition Report (SAR) (Los Angeles, CA, March 18, 2015), 11, accessed on November 19, 2016, http://www.dod.mil/pubs/foi/Reading_Room/Selected_Acquisition_Reports/16-F-0402_DOC_17_EPS_DEC_2015_SAR.pdf.

²⁵ Cristina T. Chaplain, “Space Acquisitions: Some Programs Have Overcome Past Problems, but Challenges and Uncertainty Remain for the Future,” § sec. Subcommittee on Strategic Forces, Committee on Armed Services (2015), sec. Subcommittee on Strategic Forces, Committee on Armed Services, 6, accessed on October 22, 2016, <http://www.gao.gov/assets/670/669930.pdf>.

²⁶ Holly Zell, “Impacts of Strong Solar Flares,” NASA, June 7, 2013, accessed November 9, 2016, http://www.nasa.gov/mission_pages/sunearth/news/flare-impacts.html.

natural phenomena or human interference could damage SATCOM systems—civilian or military—to a point of critical dysfunction.

Geomagnetic storms are a significant concern for any system that relies on electronics, but particularly for satellites exposed in space. The 1859 Carrington Event—a geomagnetic solar storm “with the energy of 10 billion atomic bombs”—caused telegraph machines to spark, “shocking operators and setting papers ablaze.”²⁷ A repeat of the Carrington Event on today’s digitized planet almost occurred on July 23rd, 2012, when a solar storm crossed the earth’s orbital path, missing the planet by about a week.²⁸ In *Space Weather*, Pete Riley predicts there is a 12% chance of another CME hitting the earth in the next decade with the same magnitude as the Carrington Event.²⁹ This is enough to concern a force that relies so heavily on SATCOM. If such an event were to occur, satellites would be the first to get hit, with significant disruption to their onboard electronics.³⁰ Although such an event would also affect terrestrial communication systems, they could be replaced more easily than orbiting communication satellites. Down on earth, the chaos resulting from dysfunctional security, economic, and emergency systems would be catastrophic. If the US Army had to deploy and fight amidst such chaos, the likely absence of SATCOM would leave force commanders without the means to command and synchronize forces, if they could even make it to the theater of operations.

Unavoidable CMEs are a valid concern, but intentional human interference with SATCOM is a more pressing matter. The People’s Liberation Army (PLA) of China recognizes “the United

²⁷ Christopher Klein, “A Perfect Solar Superstorm: The 1859 Carrington Event,” *History in the Headlines*, March 14, 2012, accessed November 12, 2016, <http://www.history.com/news/a-perfect-solar-superstorm-the-1859-carrington-event>.

²⁸ Tony Phillips, “Near Miss: The Solar Superstorm of July 2012,” *NASA*, July 23, 2014, https://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm.

²⁹ Pete Riley, “On the Probability of Occurrence of Extreme Spaceweather Events,” *Space Weather* 10 (2012): 1, accessed November 13, 2016, <http://onlinelibrary.wiley.com/doi/10.1029/2011SW000734/epdf>.

³⁰ Zell, “Impacts of Strong Solar Flares.”

State's high reliance on military space systems as a potential 'Achilles heel,'"³¹, and has been researching and developing counter-space and ASAT capabilities since the 1960s.³² In the early 1990s, PLA writings "drew attention to U.S. dependence on a sanctuary in space" and "discussed several alternative systems for destruction or neutralization of U.S. military space assets."³³ Several Chinese universities have developed models for "space intercept control and terminal guidance systems"³⁴ to facilitate satellite attack. At the strategic level, China's political and military elite clearly believe in the "inevitability of space militarization"³⁵ and are developing capabilities to challenge US access to space.

In January of 2007, China demonstrated its ability to target space assets by destroying their own Feng Yun 1C weather satellite at an altitude of 865 km with an ASAT missile.³⁶ This event only proved China's capability to destroy satellites in low-earth orbit (LEO), such as imaging satellites. It did not necessarily prove China's capability to destroy communications satellites in geosynchronous-earth orbit (GEO; see Figure 3). However, a 2016 Department of Defense (DoD) report explained that in 2013 "China launched an object into space on a ballistic trajectory with a peak altitude above 30,000 km, which could have been a test of technologies with a counterspace mission in geosynchronous orbit,"³⁷ allowing the targeting of communications satellites. Such

³¹ Chapman, *Space Warfare and Defense*, 203–4.

³² Michael Pillsbury, "China's Military Strategy toward the US: A View from Open Sources" (Air University Press, 2001), 20, accessed November 2, 2016, <http://www.au.af.mil/au/awc/awcgate/china/strat.pdf>.

³³ Pillsbury, "China's Military Strategy toward the US," 8.

³⁴ Ibid, 20.

³⁵ Huang Wen-Chi, "China's Space Capabilities and Their Regional Security Implications" (US Army War College, 2011), 55.

³⁶ Chapman, *Space Warfare and Defense*, 85.

³⁷ Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016" (Washington, DC, 2016), 37, <http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf>.

efforts have caused concern in the US intelligence community that China's counter-space capabilities "could destroy or disable US satellites responsible for handling nearly 90% of US military communications."³⁸ A 2006 DoD report determined that China "can currently destroy or disable satellites by launching a ballistic missile or space-launched vehicle armed with a nuclear weapon,"³⁹ causing the destruction of a cluster of satellites at a specific longitude. The strategic advantage of using a nuclear weapon in space against communications satellites is that it would paralyze the targeted nation's ability to communicate at all levels of operations without direct loss of life to the adversary's population or military personnel. Such an attack on US SATCOM would likely not result in nuclear retaliation and mutually assured destruction.

³⁸ Chapman, *Space Warfare and Defense*, 85.

³⁹ Office of the Secretary of Defense, "Annual Report to Congress: Military Power of the People's Republic of China 2006" (Washington, DC, 2006), 35, accessed on November 25, 2016, <http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf>.

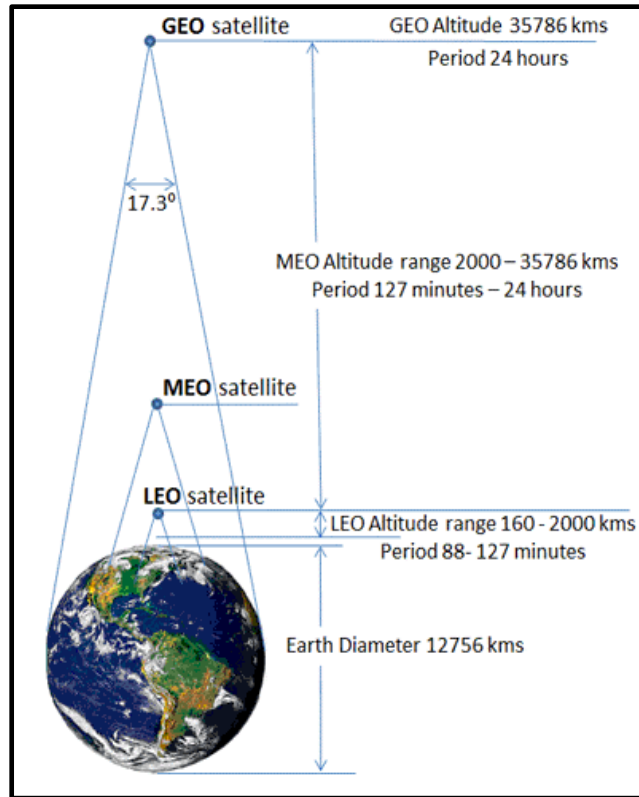


Figure 3. Satellite Orbits, Periods and Footprints “Satellite Technology Challenges,” Electropaedia, accessed November 29, 2016, <http://www.mpoweruk.com/satellites.htm>.

The PLA continues to pursue the development of directed energy weapons to augment its ASAT capability. A 2015 report by the US-China Economic and Security Review Commission (USCC) claimed that the PLA is developing “radio frequency weapons, which are designed to damage or destroy electronic components of satellites by either overheating or short-circuiting...satellites in all orbits.”⁴⁰ A 2016 DoD report predicted that China will continue to acquire “a range of technologies to improve China’s counterspace capabilities,” in the form of satellite jammers and directed energy weapons.⁴¹ As well, a Defense Intelligence Agency (DIA)

⁴⁰ USCC, “2015 Report to Congress of the U.S.-China Economic and Security Review Commission,” 2015, 298, accessed November 13, 2016, http://www.uscc.gov/Annual_Reports/2015-annual-report-congress.

⁴¹ Office of the Secretary of Defense, “Annual Report to Congress,” 2016, 37.

report confirmed that China had satellite jammers in development as well as other non-kinetic counter-space capabilities.⁴²

The USCC report also provided detailed analysis of Chinese developments of co-orbital satellites. This capability would in essence allow one satellite in orbit to “attack” another:⁴³

In June 2010, China launched the SJ-12 satellite. Over the next two months, the satellite conducted a series of maneuvers and came within proximity of the SJ-6F, an older Chinese satellite that was placed into orbit in 2008. The activities of the SJ-12 may have been designed to test a co-orbital antisatellite capability, such as on-orbit jamming. Moreover, during its maneuvers, the SJ-12 apparently bumped the SJ-6F, causing it to drift slightly from its orbital regime. This activity suggests China also could have used the test to demonstrate the ability to move a target satellite out of its intended position by hitting it or attaching to it.⁴⁴

This technological development is significant because it allows the PLA to target multiple satellites in a somewhat covert and surgical manner, preventing collateral damage to their own satellites. The report went on to illustrate:

In July 2013, China launched a rocket carrying the CX-3, SY-7, and SJ-15 satellites, one of which was equipped with a robotic arm for grabbing or capturing items in space. Once all three were in orbit, the satellite with the robotic arm grappled one of the other satellites, which was acting as a target satellite. The satellite with the robotic arm then changed orbits and came within proximity of a separate satellite, the SJ-7, an older Chinese satellite that was orbited in 2005. Robotic arms can be used for civilian missions such as satellite repair, space station construction, and orbital debris removal; they also can attach to a target satellite to perform various antisatellite missions.⁴⁵

With these developments ongoing, the US Army can expect to operate with contested access to SATCOM in a conflict with China.

Russia has been historically competitive with the US in counter-space development.

Between 1968 and 1971, Russia conducted seven ASAT tests, five of which successfully destroyed

⁴² Michael T. Flynn, “Annual Threat Assessment,” § sec. Senate Armed Services Committee (2014), sec. Senate Armed Services Committee 15, accessed on November 25, 2016, http://www.dia.mil/Portals/27/Documents/News/2014_DIA_SFR_SASC_ATA_FINAL.pdf.

⁴³ USCC, “2015 Report to Congress,” 294.

⁴⁴ *Ibid.*, 295.

⁴⁵ *Ibid.*

satellites at altitudes of 230 to 1,000 kilometers.⁴⁶ In a 2015 statement to the Senate Armed Services Committee, DIA director Lieutenant General Vincent R. Stewart warned that today “Russian leaders openly assert that the Russian armed forces have antisatellite weapons and conduct antisatellite research.” Russia recently proved its capabilities by launching the *Nudol* direct ascent missile in May 2016, which is capable of destroying communication satellites.⁴⁷ Russia tested this capability again in December of 2016 with its third successful launch of the *Nudol* from a base in central Russia.⁴⁸ Like the PLA, Russia also possesses the non-kinetic option to jam communication satellites.⁴⁹

Commercial satellites augment military communication satellites by providing flexibility to US forces operating in austere environments with little to no communications infrastructure. At the height of operations in Iraq and Afghanistan, the limited military communications structure needed this civilian augmentation. It can take up to a decade to put a military satellite constellation in orbit, but the market of commercial satellites is readily available. Commercial bandwidth is so practical that up to 90% of military satellite communication is through commercial vendors.⁵⁰ In 2011, the DoD spent over \$1 billion on commercial SATCOM services.⁵¹

⁴⁶ Chapman, *Space Warfare and Defense*, 190.

⁴⁷ Charlie Moore, “Russia Successfully Tests Anti-Satellite Missile,” *Daily Mail*, May 27, 2016, <http://www.dailymail.co.uk/news/article-3612851/Russia-successfully-tests-anti-satellite-missile-capable-wiping-navigation-communications-intelligence-devices.html>.

⁴⁸ Bill Gertz, “Russia Conducts Fifth Test of New Anti-Satellite Missile,” *Washington Free Beacon*, accessed January 19, 2017, <http://freebeacon.com/national-security/russia-conducts-fifth-test-new-anti-satellite-missile/>.

⁴⁹ Ronald C. Wilgenbusch and Alan Heisig, “Command and Control Vulnerabilities to Communications Jamming,” *Joint Forces Quarterly*, no. 69 (Quarter 2013): 58.

⁵⁰ Wilgenbusch and Heisig, “Command and Control Vulnerabilities to Communications Jamming,” 57.

⁵¹ United States Government Accountability Office, “Defense Satellite Communications: DOD Needs Additional Information to Improve Procurements” (Washington, DC, 2015), 2.

Unfortunately, commercial satellite companies outside the United States are at risk of state manipulation. From 2012 to 2014, the DoD leased the Chinese Apstar-7 satellite to increase bandwidth for US Africa Command (AFRICOM).⁵² Use of communications satellites from companies that are controlled by potentially belligerent governments leaves the US communications network vulnerable to monitoring and disruption. Also, because the data going through non-US satellites is encrypted, prolonged exposure of such sensitive communications could provide Chinese intelligence agents valuable insight into US military encryption technology.⁵³ Besides the threat of a state or private company intentionally meddling in US military communication traffic, state neutrality in a time of war may prevent some SATCOM vendors from providing the commercial bandwidth upon which US troops so heavily rely, thus disrupting force projection and operational tempo.

Lack of SATCOM Redundancy

Given potential adversaries' capability to destroy, damage, or disrupt both military and commercial SATCOM, it is important to recognize the lack of redundancy in the satellite constellations themselves. Only three satellites make up military's AEHF constellation,⁵⁴ and their Wideband Global SATCOM (WGS) system currently consists of six satellites in orbit.⁵⁵ Although there are over a thousand functioning satellites orbiting the earth, only a limited number are communications satellites. Of those, only so many can both provide sufficient bandwidth and orbit

⁵² Douglas L. Loverro, "Statement of Mr. Douglas L. Loverro Deputy Assistant of Secretary of Defense for Space Policy," § sec. Senate Committee on Armed Services Subcommittee on Strategic Forces (2014), sec. Senate Committee on Armed Services Subcommittee on Strategic Forces 12, http://www.armed-services.senate.gov/imo/media/doc/Loverro_03-12-14.pdf.

⁵³ Noah Shachtman, "Pentagon Paying China — Yes, China — To Carry Data," *Wired*, accessed November 4, 2016, <https://www.wired.com/2013/04/china-pentagon-satellite/>.

⁵⁴ Chapman, *Space Warfare and Defense*, 139.

⁵⁵ Chaplain, *Space Acquisitions: Some Programs Have Overcome Past Problems, but Challenges and Uncertainty Remain for the Future*, sec. Subcommittee on Strategic Forces, Committee on Armed Services. 8.

at the appropriate longitudinal position to provide redundancy in the event one is lost. When the DoD decided to lease the Chinese Apstar-7, it was the only available commercial communications satellite with the appropriate bandwidth and longitudinal position to support AFRICOM's communication requirements.⁵⁶ Likewise, military communication satellites are not all interchangeable with regard to bandwidth capacity and orbital position.

Even if just a single US communications satellite were to be destroyed, it could have devastating effects on communications for land forces.⁵⁷ Because a single AEHF satellite can support up to 6,000 terminals,⁵⁸ loss of one satellite could result in thousands of ground terminals immediately losing the ability to communicate with their headquarters beyond line-of-sight range. Ground units would continue to lack communication until either they switched to a redundant satellite (if available), until they adopted a terrestrial CNR solution, or until the US put a new satellite in orbit.

Replacing satellites is a lengthy and expensive process. For example, the first AEHF satellite was scheduled for launch in 2006, but did not actually launch until 2010. The second AEHF satellite went into orbit in 2012, five years later than its original launch date. Besides the emplacement time, satellites are expensive. The total AEHF program cost is currently at \$14.6 billion, which is twice the original cost estimate.⁵⁹ The United State's acute reliance on communication satellites in war could come with significant replacement costs in time and money. This liability during a resource-constrained war could paralyze US communication and allow the swift defeat of US forces.

⁵⁶ Shachtman, "Pentagon Paying China — Yes, China — To Carry Data."

⁵⁷ Deakin, *Battlespace Technologies*, 324.

⁵⁸ Chapman, *Space Warfare and Defense*, 139.

⁵⁹ Chaplain, Space Acquisitions: Some Programs Have Overcome Past Problems, but Challenges and Uncertainty Remain for the Future, sec. Subcommittee on Strategic Forces, Committee on Armed Services 6.

The US Army does recognize this dependence and is developing and fielding systems to fill the gap with terrestrial systems such as High-band Networking Waveform (HNW) and Mid-Tier Networking Vehicular Radio (MNVR). HNW is meant to allow Army command and control systems to continue to function if SATCOM is lost, without significantly sacrificing rates of data. Unfortunately, the most recent Follow-on Operational Test and Evaluation (FOT&E) of the HNW yielded disappointing results. At best, the HNW could achieve ranges of 10 km in the open desert—with use of a stationary relay tower—but even at these short distances, 81% of data traffic still went through SATCOM. The evaluation document also reported that the HNW was limited to distances of 1 km in the densely wooded terrain of Ft. Campbell, Kentucky.⁶⁰

MNVR is capable of providing terrestrial communication for the Joint Battle Command-Platform (JBC-P), which is primarily driven by SATCOM. However, an evaluation in 2013 determined that the MNVR was “not operationally suitable due to poor reliability.”⁶¹ During testing in 2015, MNVR was not capable of sending messages at distances as short as six to ten kilometers, and in degraded SATCOM environments, it did not meet the message completion requirement of “90 percent at-the-halt and 85 percent on-the-move.”⁶² Even though the US Army is making efforts to build terrestrial redundancy in the event of SATCOM loss, it is unlikely that it will fix the SATCOM dependence any time soon.

Overreliance on SATCOM will surely pose some of the above challenges to an army at war. To fight effectively, US ground forces must have mission command systems that can function through mediums other than SATCOM. Although many consider SATCOM to be critical to the

⁶⁰ Director, Operational Test and Evaluation, “Warfighter Information Network-Tactical (WIN-T) Increment 2, Second Follow-on Operational Test and Evaluation,” 2015, iii.

⁶¹ Sydney J. Freedberg Jr., “Army Radios Get Low Marks From DOTE,” *Breaking Defense*, January 29, 2014, accessed on November 25, 2016. <http://breakingdefense.com/2014/01/army-radios-get-low-marks-from-dote/>.

⁶² Director, Operational Test and Evaluation, “FY 2015 Annual Report,” 136.

function of US operations, SATCOM may be significantly degraded or eliminated to the point that commanders *must* rely on terrestrial communications. In order to continue the fight, US forces will have to increasingly rely on terrestrial CNR, which comes with its own set of challenges.

Terrestrial Communication: Increased Need and Renewed Threat

In a conflict where access to SATCOM is contested, ground elements—from individual vehicles all the way up to corps-level headquarters—will likely increase their use of terrestrial CNR. A corresponding increase in electronic signature will raise their exposure to terrestrial EW threats. The US Army has a strong historical and doctrinal precedent for countering these threats. Unfortunately, potential adversaries of the US have increased their ability to target terrestrial CNR through direction finding and electronic countermeasures (ECM)⁶³ such as jamming. Meanwhile, the US Army’s confidence in its terrestrial systems’ survivability against EW has allowed US ground forces to become complacent and to develop communication practices that lack proper emphasis on countering these threats through electronic counter-countermeasures (ECCM).⁶⁴ The Army has also developed communication networks that increase the electronic signatures of ground elements, exposing them to an enemy with increasingly precise sensors and weaponry.

A Precedent for Emission Control

Both jamming and direction finding are significant concerns for ground force communication. Jamming is dangerous in that it prevents units from communicating (i.e. preventing the calling of a much-needed reserve, calling for artillery support, logistics support, etc.), but jamming does not provide to the threat a location of friendly positions. Direction finding is

⁶³ James M. Rockwell, ed., *Tactical C³ for the Ground Forces*, AFCEA/SIGNAL Magazine C³I Series, v. 4 (Washington, DC: AFCEA International Press, 1986), 293. ECMs are “those actions taken to prevent effective use of the electromagnetic spectrum by an enemy (includes jamming and deception).”

⁶⁴ Ibid. ECCMs are “those actions taken to insure effective friendly use of the electromagnetic spectrum (despite hostile ECM efforts).”

significantly dangerous because even the most rapid transmission can allow the enemy to locate friendly command nodes or force concentrations. The enemy can then target the friendly force with indirect fires or air attack within minutes. When two separate enemy direction finders attain lines of bearing on a radio emitter, the intersection of those two lines forms a “cut.” When three or more bearings are attained, the intersection of those lines is called a “fix” (See Figure 4). The 1987 Field Manual (FM) 24-18, *Tactical Single-Channel Radio Communication Techniques*, states that if enemy direction finders are within 20-25 kilometers of the front line, they can normally attain a fix on the emitter with a 90% circular error probable (CEP)⁶⁵ of 1,500 meters. Today, some Russian direction finders have a direction of arrival (DOA) accuracy of one degree.⁶⁶ With this accuracy, two Russian direction finders could locate a friendly emitter 20 km away with a 500 meter 90% CEP. If 10 km away, the 90% CEP would be 170 meters.⁶⁷ Most “Threat forces” will fire on a 90%

⁶⁵ David Adamy, *EW 103: Tactical Battlefield Communications Electronic Warfare* (Boston, MA: Artech House, 2009), 195. Ninety percent CEP is the radius of circular area with a “90% chance of containing the true emitter.”

⁶⁶ Lester W. Grau and Charles K. Bartles, “The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces (Draft)” (Ft. Leavenworth, KS: Foreign Military Studies Office, 2016), 243.

⁶⁷ Adamy, *EW 103*, 197. Adamy’s formula is $90\% \text{ CEP} = 1.57d \tan (\text{RMS})$. Where d is the direction finder distance in kilometers to the emitter and RMS (root mean square) is the error of the direction finders accuracy in degrees.

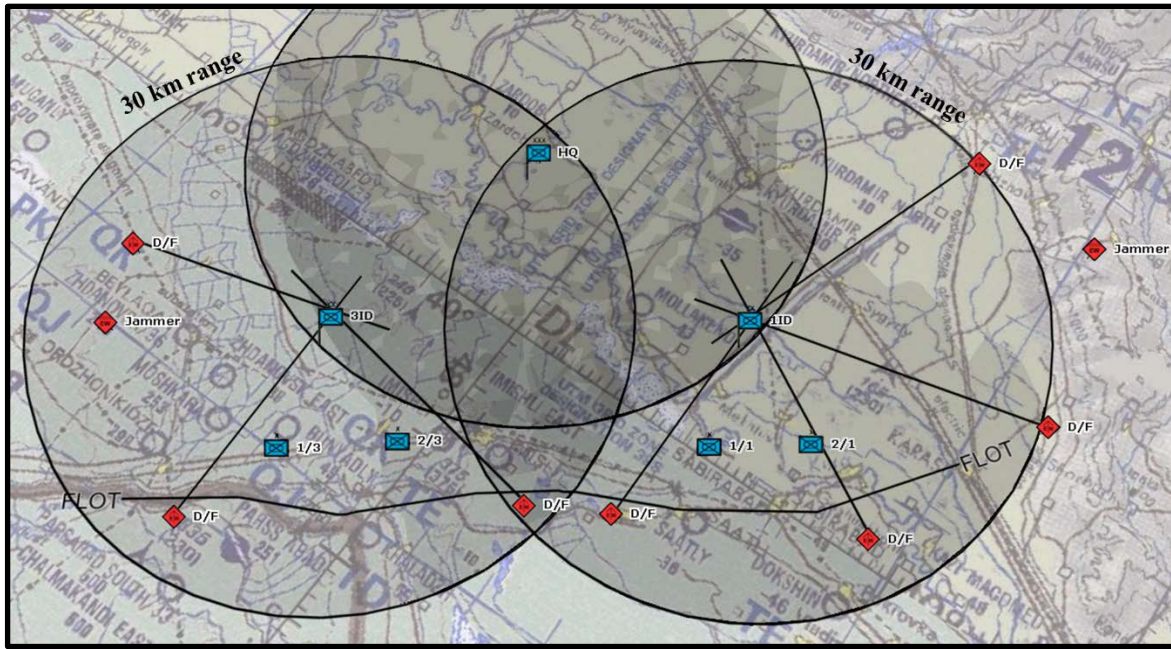


Figure 4. Notional direction finding of division command posts in Azerbaijan. Enemy direction finders (D/Fs) acquire fixes on friendly command posts that are emitting at maximum range and in all directions. Created by the author using the National Geospatial-Intelligence Agency ONC “Base Background Map, 1:1,000,000.”

CEP if they have sufficient artillery.⁶⁸ Through terrain analysis, the enemy can refine the precise location of the friendly emitter within that CEP, since most emitters will be located on high terrain to achieve line-of-sight communication with adjacent forces. The enemy could also use these CEPs to cue an unmanned aerial sensor to attain the exact location of the targeted emitter.

Direction finding is not limited to horizontal triangulation, because HF direction finders add a vertical dimension to the geometry. A particular advantage of an HF direction finder is that it can use single-site location (SSL) with only *one* bearing to determine the location of the emitter.⁶⁹ Because long-range HF transmissions bounce off the ionosphere, an SSL direction finder receives an azimuth and an elevation angle of arrival from the source of emission. Because the height of the ionosphere is known, the distance to the direction finder is easily triangulated (see Figure 5).

Simply coupling the direction with the distance provides a general location of the emitter, at which

⁶⁸ Field Manual (FM) 24-18, *Tactical Single-Channel Radio Communication Techniques* (Washington, DC: Government Printing Office, 1987), 6-2.

⁶⁹ Adamy, *EW 103*, 190–91.

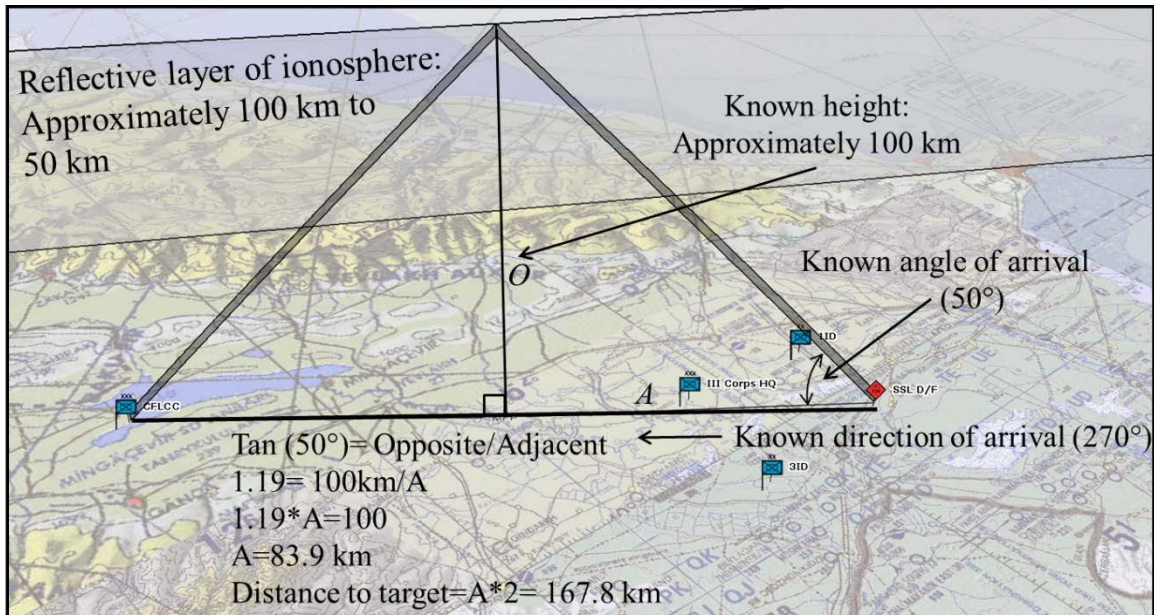


Figure 5. Notional single-site location (SSL) in Azerbaijan. Created by the author using the National Geospatial-Intelligence Agency ONC “Base Background Map, 1:1,000,000.”

point additional sensors can refine the precise location for targeting. In a conventional war with contested access to space, ground elements will have to rely more on HF ionospheric refraction for long-range communication. Although direction finding using horizontal triangulation has more historical precedent, SSL is especially concerning for US forces if HF is one of the only long-range communication alternatives to SATCOM.

The British Army employed direction finding during World War I as early as 1914, providing the capability to locate German transmitters. By 1915, the British could identify even low-power transmitters along the German trenches as well as the routes of airships on their way to raid Great Britain.⁷⁰ The French also made use of direction finding in World War I, and were successful enough to “develop the [German] order of battle, track their forces as they moved, and

⁷⁰ John M. Carroll, *Secrets of Electronic Espionage* (New York, NY: EP Dutton & Co., Inc., 1966), 25–26.

determine their intent,” allowing the French army to halt the Germans at the Battle of the Marne.⁷¹ When the American Expeditionary Force (AEF) entered the war, their radio intelligence sections used direction finding to discern the German order of battle through traffic analysis.⁷² The US Army continued to employ direction finding during World War II, and army-level fronts in the European Theater of Operations often employed up to twelve direction finding stations on a thirty-five mile front.⁷³

To avoid threat direction finding, emission control is the most basic method. Emission control is achieved when transmissions are reduced to short “chirps,” when the power and direction of transmission is reduced, or when “radio silence” is broadly enforced.⁷⁴ During World War II, controlling radio emissions became a significant concern for both the Allied and Axis powers. To avoid the allied direction finding in the Atlantic at the end of 1943, the German submarine crews began pre-recording messages prior to transmission, would speed up the recording, and then would transmit the accelerated message in a fraction of a second, denying a directional bearing to allied direction finders. The German receiver—be it another submarine or a land-based headquarters—would then record the transmission, and then speed up the transmission for “normal listening.”⁷⁵

⁷¹ Jeffrey S. Harley, “Reading the Enemy’s Mail: Origins and Development of US Army Tactical Radio Intelligence in World War II, European Theater of Operations” (US Army Command and General Staff College, 1993), 8.

⁷² Jeffrey S. Harley, “Reading the Enemy’s Mail,” 11; Traffic Analysis: when a transmitter (from an enemy regimental headquarters) behind the front lines would send a message, three separate transmitters (subordinate headquarters) would sequentially respond. This indicated to the signal intelligence section that the three “forward” transmitters were subordinate to the transmitter that was behind the front line, allowing the estimation of the enemy order of battle.

⁷³ Laurie G. Moe Buckhout, “Signal Security in the Ardennes Offensive: 1944-1945” (US Army Command and General Staff College, 1997), 31, accessed on October 12, 2016, <http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll2/id/829>.

⁷⁴ Abdul Karim Baram, *Technology in Warfare: The Electronic Dimension* (Abu Dhabi, UAE: The Emirates Center for Strategic Studies and Research, 2008), 409.

⁷⁵ Abdul Karim Baram, *Technology in Warfare: The Electronic Dimension*; coinciding with this German ECCM, the Allies developed an improved direction finder called Huff-Duff, which was able to calculate directions of even these short, rapid transmissions.

The Soviet Army also used emission control on the Eastern Front for the purpose of avoiding German direction finders and other forms of radio reconnaissance. Learning from their lack of radio discipline during World War I and consequential defeat at Tannenberg, the Russians enforced strict emission control to deny the Germans the opportunity to triangulate Russian positions.⁷⁶

The US Army also took ECCM seriously during World War II. Eighth Army Field Order 17 for the 1944 invasion of Luzon directed strict radio silence to be lifted only when surprise was completely lost, or when the “leading wave of troops crosses the line of departure.” The order also directed that when radio silence was lifted, units were restricted to using 15 watt radios, which limited reception by distant enemy sensors.⁷⁷ A 6th Infantry Division order, from the same amphibious assault at Luzon, also emphasized appropriate emission control, directing that radio silence for radios above 15 watts would be lifted only when “directed by this headquarters.” To reduce radio traffic, the order committed an entire paragraph to the proper use of messenger pigeons on patrol, directing that “Maximum use of pigeons will be made when practical.”⁷⁸ A 5th Army outline plan for Operation Shingle, the invasion of Anzio, was just as insistent on radio silence:

Radio silence will be observed until H minus 30 minutes at which time the Rangers and Paratroops will attack. In dire circumstances radio silence may be broken (as during an air Attack) but only to the extent required to cope with the situation.⁷⁹

⁷⁶ David Kahn, *Hitler's Spies: German Military Intelligence in World War II* (New York: Macmillan, 1978), 451.

⁷⁷ Headquarters, Eighth Army, US Army, “Field Order 17, Annex 5,” January 22, 1945, 6, accessed December 2, 2016, <http://cgsc.cdmhost.com/cdm/singleitem/collection/p4013coll8/id/3064/rec/2>.

⁷⁸ Headquarters, 6th Infantry Division, US Army, “Field Order 1, Annex XIII,” November 28, 1944, 6, accessed December 2, 2016, <http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll8/id/29>.

⁷⁹ Headquarters, 5th Army, US Army, “Outline Plan, Operation Shingle, Air Plan Communications,” January 12, 1944, 5, accessed December 2, 2016, <http://cgsc.cdmhost.com/cdm/singleitem/collection/p4013coll8/id/3942/rec/1>.

One way around such strict use of radio silence (and pigeons) was the Army's increased use of directional antennas. If a headquarters knows the general direction of the receiving friendly radio station, it can point a directional antenna in that general direction, instead of emitting a signature in all directions, which may include the enemy's sensors. Units on the front line can focus their antennas toward their parent headquarters, and parent headquarters can focus their antenna to cover only the left and right limits of their subordinate formations. A 1975 Army Command and General Staff College monograph explained that the use of directional antennas would provide additional range while avoiding enemy EW assets.⁸⁰ At the time of that writing, the US Army took communications EW seriously enough that it developed a standardized directional log period antenna to mitigate these threats.⁸¹ FM 24-18, published in 1987, described the science of radio theory in detail, provided an entire chapter on how to communicate effectively in the presence of EW threats, and put strong emphasis on the use of directional antennas to avoid enemy jamming and elude enemy direction finding.⁸²

Another method the Army developed during the Cold War to avoid enemy EW assets was called null steering. The Steerable Null Antenna Processor (SNAP-1), fielded in the mid-1980s, manipulated the frequencies of two antennas from the same radio to cancel out signals in the direction of an enemy jammer.⁸³ In addition to avoiding unwanted jamming signals, the friendly radio site could also "null out" their signal in the direction of suspected enemy direction finders, denying them a line of bearing.⁸⁴ The use of null steering provided a significant benefit because it

⁸⁰ Robert D. Rood, "FM Tactical Communications under Intentional Interference" (US Army Command and General Staff College), 39, accessed October 4, 2016, <http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll2/id/1354>.

⁸¹ Ibid.

⁸² Field Manual (FM) 24-18, *Tactical Single-Channel Radio Communication Techniques*.

⁸³ Ibid, E-1.

⁸⁴ Adamy, *EW 103*, 59–60.

maintained simplicity with 360-degree directional communication, but could still automatically adjust to account for jamming or direction finding. The SNAP-1 was only capable of communicating through the single-frequency setting on SINCGARS, but the SNAP-2 was under development to function with SINCGARS' frequency-hopping mode.⁸⁵ Another system used in the

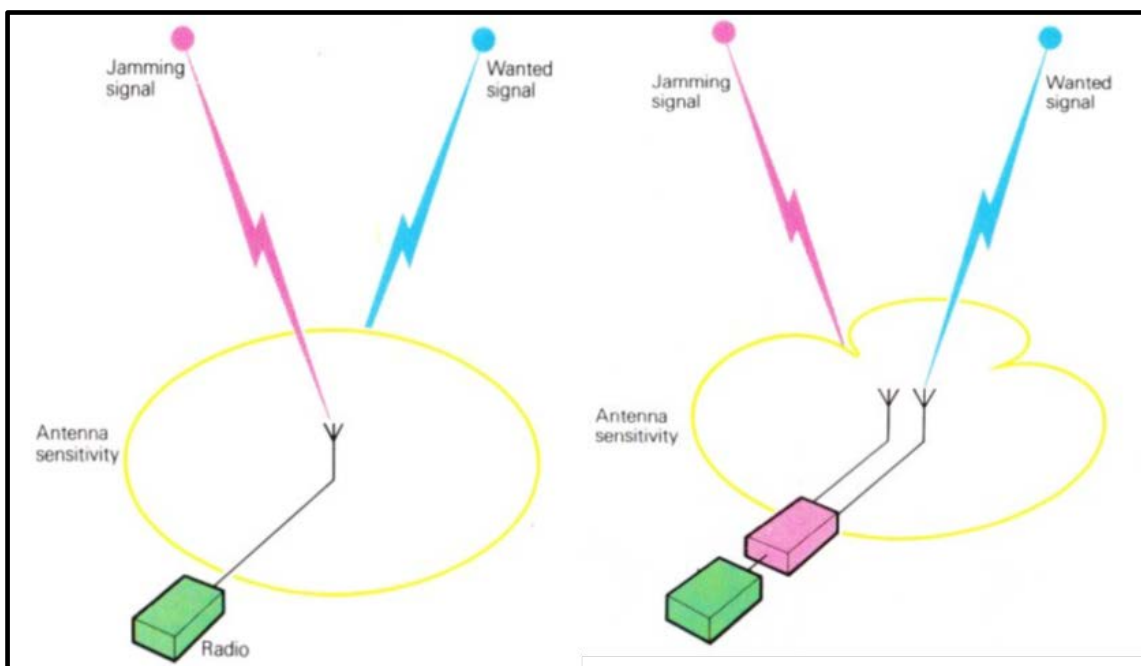


Figure 6. Plessey Interference Cancellation System. Doug Richardson, *An Illustrated Guide to the Techniques and Equipment of Electronic Warfare* (New York, NY: Arco Pub, 1985), 69.

1980s was the Plessey Interference Cancellation Equipment (ICE; See Figure 6), which operated on the same principle. Through the ICE, the radio could reduce “sensitivity in the direction of the jammer,” and increase “reception of the wanted signal.”⁸⁶ Some null steering concepts are currently in use or in development for applications such as aerial communications and GPS anti-jamming, but null steering is not a typical technique in US Army communications ECCM.

⁸⁵ Field Manual (FM) 24-18, *Tactical Single-Channel Radio Communication Techniques*, E-1. It is unknown if the SNAP-2 is still in inventory.

⁸⁶ Doug Richardson, *An Illustrated Guide to the Techniques and Equipment of Electronic Warfare* (New York, NY: Arco Pub, 1985), 69.

Historical, doctrinal, and technological precedent shows that the US Army had a healthy concern for a defensive electronic posture during the Cold War. In this context, the US Army continued to pursue technological improvement in electronic protection. The US military began design of SINCGARS in 1974, with production deliveries starting in 1988.⁸⁷ SINCGARS replaced many of the Vietnam-era radios that were considerably vulnerable to electronic interception and jamming. The advantage of SINCGARS—both in the 1980s and today—is that it can change frequencies over 100 times per second on a hopping pattern known only to friendly radio systems.⁸⁸ Older enemy direction finders and jammers that are mechanically tuned cannot keep up with the automated speed of such ECCM.⁸⁹ Coinciding with the use of SINCGARS, the US Army began fielding EPLRS in 1987.⁹⁰ EPLRS uses frequency hopping and time division multiple access,⁹¹ whereby each EPLRS radio “chirps” its positioning and messaging data in an allotted timeframe of 1.95 milliseconds,⁹² being quite elusive to electronic sensors. These developments gave the US Army an edge of confidence in ECCM technology.

Apathy towards a Renewed EW Threat

The advances in ECCM technology in the 1980s and the decline of the Soviet Union allowed the US Army to relax its emphasis on the EW threat. During the 1991 Persian Gulf War, the Iraqi Army enforced strict radio silence until in contact with the enemy, but the US-led coalition

⁸⁷ Sterling, *Military Communications*, 412.

⁸⁸ Field Manual (FM) 6-02.72, *Tactical Radios*, I-2.

⁸⁹ Adamy, *EW 103*, 157.

⁹⁰ Roland Proesch, *Technical Handbook for Radio Monitoring VHF/UHF* (Germany: Books On Demand, 2013), 174.

⁹¹ Deakin, *Battlespace Technologies*, 386.

⁹² Frater and Ryan, *Electronic Warfare for the Digitized Battlefield*, 42; Simulation Interoperability Standards Organization EPLRS/SADL Product Development Group (PDG), “Enhanced Position Locating Reporting System (EPLRS)” (Orlando, FL: Simulation Interoperability Standards Organization (SISO), Inc., 2013), 9.

found it difficult to maintain radio discipline.⁹³ Despite inferior emission control, the coalition's overwhelming force prevailed, and the Iraqi Army quickly retreated from Kuwait. Following the US Army's impressive performance in the Gulf War, the Soviet Union collapsed, marginalizing the US Army's most formidable competitor on the electromagnetic spectrum and warfare in general. US Army doctrine gradually began to assume a dependable advantage over enemy ECM. In 1996, FM 11-1, *Talk II-SINCGARS*, claimed that with the fielding of SINCGARS, the "capabilities of sophisticated, complex enemy jammers have to a great extent been neutralized," even considering the "technological improvements in enemy jamming and electronic collection" at that time.⁹⁴ With the end of the Cold War, the US military went through what would later be called "twenty-five years of EW neglect."⁹⁵

A comparison of doctrine from the 1980s with that of today shows the clear disparity in emphasis on electronic protection. In 1987, FM 24-18 devotes an entire chapter to an adversary's intentions and capabilities regarding the interdiction of friendly communication. The chapter dedicated eight pages of EW considerations and techniques for the employment of tactical radios. The manual details critical aspects of enemy interception, direction finding, jamming, and techniques for radio operators to overcome jamming with various radio sets. In addition to having a section completely dedicated to ECCM, the manual references ECCM seventeen times. The manual provides an entire annex dedicated to the use of the SNAP-1. The manual explains in detail the inherent advantage of additional gain and avoidance of enemy jammers and direction finders.⁹⁶

⁹³ Baram, *Technology in Warfare*, 409.

⁹⁴ Field Manual (FM) 11-1, *Talk II-SINCGARS* (Washington, DC: Government Printing Office, 1996), vii.

⁹⁵ Defense Science Board, "21st Century Military Operations in a Complex Electromagnetic Environment" (Washington, DC, July 2015), 6, accessed on November 14, 2016, http://www.acq.osd.mil/dsb/reports/DSB_SS13--EW_Study.pdf.

⁹⁶ Field Manual (FM) 24-18, *Tactical Single-Channel Radio Communication Techniques*.

More recent doctrine does not share such emphasis on the EW threat. Army Techniques Publication (ATP) 6-02.72, *Tactical Radios*, discusses ECCM only three times, directional antennas once, and null steering not at all.⁹⁷ FM 6-02, *Signal Support to Operations*, does not mention directional antennas, emission control, nor ECCM, but it at least mentions EW three times. FM 11-45, *Signal Support to Theater Operations*, mentions EW a single time, but jamming, emission control, ECCM are completely omitted.⁹⁸ In Field Manual Interim (FMI) 6-02.45, *Signal Support to Theater Operations*, EW is mentioned three times and emission control only once.⁹⁹ After years of confidence in technological superiority and minimal EW threat to the US Army, the current doctrine does not adequately address the renewed threat to communication systems.

Some in the signal community may consider ECCM less in the purview of communications doctrine and more in the realm of EW doctrine, but EW manuals are no better at including ECCM. For example, FM 3-38, *Cyber Electromagnetic Activities*, which broadly covers aspects of both cyber and EW, mentions emission control twice, but does not specifically reference ECCM at all. The manual mentions directional antennas and other forms of ECCM in passing:

Take appropriate actions to minimize the vulnerability of friendly receivers to enemy jamming (such as reduced power, brevity of transmissions, and directional antennas). Ensure redundancy in all systems is maintained and personnel are well-versed in switching between systems.¹⁰⁰

ATP 3-36, *Electronic Warfare Techniques*, mentions direction finding five times, but provides no in-depth description of how an enemy may employ direction finding, nor does it provide any

⁹⁷ Army Techniques Publication (ATP) 6-02.72, *Multi-Service Tactics, Techniques, and Procedures for Tactical Radios* (Washington, DC: Government Printing Office, 2013).

⁹⁸ Field Manual (FM) 11-45, *Signal Support to Theater Operations* (Washington, DC: Government Printing Office, 1999).

⁹⁹ Field Manual Interim (FMI) 6-02.45, *Signal Support to Theater Operations* (Washington, DC: Government Printing Office, 2007).

¹⁰⁰ Field Manual (FM) 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Government Printing Office, 2014), 4-4.

solutions for avoiding that type of detection. To be fair, at least ATP 3-36 provides a definition for “electronic masking” as:

...the controlled radiation of electromagnetic energy on friendly frequencies in a manner to protect the emissions of friendly communications and electronic systems against enemy electronic warfare support measures/signals intelligence without significantly degrading the operation of friendly systems.¹⁰¹

However, this manual for *techniques* provides no recommended *methods* for achieving electronic masking or other ECCM.

Again, the lack of emphasis on electronic protection in US Army communications and EW doctrine indicates the Army is not actively concerned about avoiding enemy electronic jammers and sensors. This is in sharp contrast with the 1987 doctrine of FM 24-18, a simple radio manual, which provides more in-depth analysis of enemy EW effects—as well as appropriate ECCM—than do all of the contemporary manuals listed above.

Part of this shift was due to a reduced EW threat. The swift defeat of the Iraqi Army, the waning military power of Russia during the 1990s, and the rapid toppling of Saddam Hussein in 2003 made security on the electromagnetic spectrum seem like an afterthought. However, the belief that SINCGARS could elude modern enemy jammers, as surmised in FM 11-1, is inaccurate. Even before the full fielding of SINCGARS in 1987, scholars were voicing the concern that it was still vulnerable to EW capabilities. A 1986 monograph bemoaned that procurement of SINCGARS radios was underway “despite the fact that it is now known that they are just as vulnerable to the new jammers as are single channel radios.”¹⁰² While SINCGARS can elude more primitive electronic sensors, today’s computer-assisted jammers and direction finders can ascertain the hop pattern of frequency hopping radios through the use of computer processors. With these advances in

¹⁰¹ Army Techniques Publication (ATP) 3-36, *Electronic Warfare Techniques* (Washington, DC: Government Printing Office, 2014), 1-2.

¹⁰² David Bolton, *The Challenge of Electronic Warfare* (London: Royal United Services Institute for Defence Studies, 1986), 30.

EW technology, frequency hopping radios now “stand out” due to their emission of unique and sporadic “frequencies at a single location.”¹⁰³ After determining the hop pattern, “a follower jammer could be assigned to the frequency associated with that location—thereby jamming every hop” of that radio.¹⁰⁴ Frequency hopping radios still have an advantage over analog EW equipment, but the improvements in threat EW technology have made frequency hopping emitters *easier* to identify when surrounded by non-military transmissions in single frequency.

The US Army treats EW as an afterthought—more of an impediment to operations than an enabler.¹⁰⁵ However, the Russian military gives EW high priority.¹⁰⁶ Today, each Russian maneuver brigade has its own EW company, while US battalions will have only two EW personnel.¹⁰⁷ Russia has sophisticated communications EW systems such as the R-330B VHF jamming and direction-finding system (see Figure 7), which can detect and jam frequency hopping emitters at up to 300 times per second (enough to keep up with SINCGARS and similar systems). It can also get a bearing on an emitter direction within 3 degrees of accuracy and has a detection-to-suppression time of less than 5 milliseconds.¹⁰⁸ In a situation where access to SATCOM is denied, use of VHF for data and voice traffic will likely rise, leaving US forces vulnerable to detection and triangulation with such systems as the R-330B.

¹⁰³ Adamy, *EW 103*, 230.

¹⁰⁴ Ibid.

¹⁰⁵ Loren Thompson, “Electronic Warfare: How The U.S. Army Could Lose Its Next War,” *Forbes*, accessed October 19, 2016, <http://www.forbes.com/sites/lorenthompson/2016/03/15/electronic-warfare-how-the-u-s-army-could-lose-its-next-war/>.

¹⁰⁶ Grau and Bartles, “The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces (Draft),” 241.

¹⁰⁷ Paul McCleary, “Russia’s Winning the Electronic War,” *Foreign Policy*, October 21, 2015, <https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/>.

¹⁰⁸ Grau and Bartles, “The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces (Draft),” 245.



Figure 7. R-330B direction finder. Lester W. Grau and Charles K. Bartles, “The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces” (Ft. Leavenworth, KS: Foreign Military Studies Office, 2016), 244.



Figure 8. R-378AM direction finder and jammer. Lester W. Grau and Charles K. Bartles, “The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces” (Ft. Leavenworth, KS: Foreign Military Studies Office, 2016), 243.

Another notable Russian EW system is the R-378AM. This system can jam and find the direction of HF radio systems (see Figure 8),¹⁰⁹ putting long-range transmitters at risk of being located through single-site location. The Organization for Security Cooperation in Europe (OSCE) has identified similar EW systems employed in eastern Ukraine in support of pro-Russian separatists.¹¹⁰ The use of such EW capabilities has caused considerable communication problems for Ukrainian forces. Ukrainian forces sometimes have to rely on hard-wired field telephones due to the frequency of Russian jamming,¹¹¹ which often leaves their cell phones and radios “unusable for hours at a time.”¹¹² For sure, the Russians are an EW threat which the US Army must address.

¹⁰⁹ Grau and Bartles, “The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces,” 244.

¹¹⁰ Organization for Security and Co-operation in Europe, Special Monitoring Mission to Ukraine, “Camouflaged ‘R-330ZH Zhitel’ Jamming Station,” 2016.

¹¹¹ Joint Multinational Training Group-Ukraine et al., “Lessons Learned from the UKR 1-24th Mech BDE” (Yavoriv, Ukraine: International Peacekeeping Security Center, April 14, 2016), 14.

¹¹² McCleary, “Russia’s Winning the Electronic War.”

The Army's lack of emphasis on communications EW coincides with the proliferation of precision-guided weaponry and unmanned aerial vehicles (UAVs) in the hands of US adversaries. For all the emphasis the Army placed on masking communication emissions during World War II, the consequence of lacking radio discipline may have only been a massed artillery bombardment. Today, however, potential adversaries have precision capability which can completely destroy headquarters and massed forces at any echelon if their location is known. Even the slightest chirp of a radio emission picked up by a single direction finder can cue an enemy UAV along a directional bearing to identify the target location, leading to the devastating accuracy of enemy precision fires. A recent account from the Russo-Ukrainian War best illustrates this potential:

The low-intensity counterinsurgency wars in Iraq and Afghanistan have not prepared U.S. forces for the high-intensity, peer-on-peer battlefield. In July 2014, Russia launched fire strikes with long-range artillery and multiple rocket launchers employing top-attack munitions and thermobaric warheads against two Ukrainian mechanized battalions in the open. This intensely concentrated fire strike lasted only a few minutes yet inflicted high casualties and destroyed most armored vehicles, rendering both battalions combat-ineffective.¹¹³

This is one of many examples that have deeply resonated with US Army leaders as a caution to prepare for a fight with a near-peer adversary, where there is no guarantee of technological superiority as there was in the Gulf War and in the 2003 invasion of Iraq. A US Army Cyber Command official claimed that “you can’t but come to the conclusion that we’re not making progress at the pace the [EW] threat demands.”¹¹⁴ General Milley described a future enemy with

¹¹³ Phillip Karber and Joshua Thibeault, “Russia’s New Generation Warfare,” *The Potomac Foundation*, May 13, 2016, accessed December 2, 2016.
<http://www.thepotomacfoundation.org/russias-new-generation-warfare-2/>.

¹¹⁴ McCleary, “Russia’s Winning the Electronic War.”

“drones and sensors constantly on the hunt for targets,” and warned that “if you stay in one place longer than two or three hours, you will be dead.”¹¹⁵

With an enemy constantly searching for signs of US forces on the electromagnetic spectrum, the US Army would likely not cultivate a doctrine that is naïve about electronic detection while procuring equipment that increases exposure to threat EW sensors. Unfortunately, this is exactly what the Army is doing. In its embrace of network-centric warfare, the Army is buying systems that create *greater* signatures on the electromagnetic spectrum. For example, Warfighter Information Network-Tactical (WIN-T) allows commanders “far from the scene [to] stay in contact with the patrol leaders and [to] rapidly communicate orders through a high-speed, high-capacity network.”¹¹⁶ This network functions through employment of the High-band Networking Waveform (HNW), the Soldier Radio Waveform, and the Wideband Networking Waveform, all of which add to the electronic footprint of US forces. Although such networks are intended to allow information superiority, they come at the high risk of increasing the exposure of US troops to threat EW sensors. The 2015 annual report from the Director, Operational Test and Evaluation (DOT&E) acknowledges the danger of such networks since they are “constantly emitting,” and “are much more vulnerable to threat electronic direction finding.”¹¹⁷

While increasing the vulnerability of US forces to threat EW sensors, WIN-T’s waveforms provide a fraction of the range and expediency that legacy radio systems offer. The same DOT&E report explains that “these waveforms, due to their higher frequencies, have shorter ranges and are more affected by terrain obstructions compared to the legacy Single Channel Ground and Airborne

¹¹⁵ Sydney J. Freedberg, “Miserable, Disobedient & Victorious: Gen. Milley’s Future US Soldier,” *Breaking Defense*, October 5, 2016, accessed on November 25, 2016, <http://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us-soldier/>.

¹¹⁶ John Antal, “Simplify, Simplify, Simplify: An Update on the US Army’s Lower Tactical Internet Effort,” *Military Technology*, February 2015, 84.

¹¹⁷ Director, Operational Test and Evaluation, “FY 2015 Annual Report,” 104.

Radio System waveform.”¹¹⁸ The HNW in particular did not function at line-of-sight ranges much beyond 10 km in the open desert of White Sands Missile Range, New Mexico. In the forested terrain of Ft. Campbell, HNW functioned up to 2.5 km, but usually lost connectivity at 1 km.¹¹⁹ This flawed pursuit of WIN-T’s terrestrial network to support the high data rates of SATCOM-dependent mission command systems decreased transmission range while increasing the exposure to threat EW sensors.

Despite these concerns—and for reasons beyond the scope of this monograph—the US Army is “committed to using networking waveforms,”¹²⁰ and the fielding of such communications technology is well underway. Information superiority is not an end in and of itself but the means to an end, and that end is successful combat operations—even in the face of EW threats. Having instantaneous information can be quite advantageous, but it should not come at the expense of reducing transmission range while broadcasting the exact locations of US formations to threat sensors.

The US Army is significantly vulnerable to terrestrial EW attack and detection. Although there is strong historical, technological, and doctrinal precedent for the US Army’s inclusion of EW defense, the most recent doctrine and equipment altogether exclude electronic protection. Russia has proved its effective EW capability against the Ukrainian Army, and the technological advantage that the US enjoyed in past conflicts will not continue against such a threat. The US Army must address its EW capability gap.

¹¹⁸ Director, Operational Test and Evaluation, “FY 2015 Annual Report,” 104.

¹¹⁹ Director, Operational Test and Evaluation, “Warfighter Information Network-Tactical (WIN-T) Increment 2, Second Follow-on Operational Test and Evaluation,” 29-30.

¹²⁰ Director, Operational Test and Evaluation, “FY 2015 Annual Report,” 104.

Recommendations

The US Army should prepare for the loss of SATCOM in a future conflict, as such a loss is sufficiently likely. Preparing for such a conflict will require systems to have the flexibility to operate through terrestrial CNR. Regardless, with or without an increased use of terrestrial CNR, the US Army is also likely to encounter significant terrestrial EW reconnaissance and attack. To prepare for this threat, the Army should make immediate changes to equipment, doctrine, and training to address the current threat.

Equipment

To equip for a future conflict with a persistent space and EW threat, the Army should cease fielding of WIN-T, develop mission command systems that can function at low data rates, field directional antennas for terrestrial communication systems, and employ null steering processors to mitigate the EW threat. The most recent tests and evaluations of WIN-T show that it will not facilitate adequate command and control of forces if space is a contested domain, while its network will also be dangerously visible to threat electronic sensors. As well, its lack of adequate transmission range is not worth whatever increase in data rate it may provide.

With contested access to space, the Army may have to rely on legacy radio systems for data transfer. The various mission command systems should have software updates to allow continued function through a “degraded mode”—through terrestrial CNR mediums—in the event of SATCOM loss. Some of this has already happened outside the formal acquisition process. For example, a unit deployed to Iraq in 2005 requested that Raytheon provide a means to transmit AFATDS data through the HF PRC-150 Harris Radio. Raytheon created a software update, burned it to a CD, and mailed it off to the unit within two weeks.¹²¹ This allowed AFATDS to function

¹²¹ Henry S. Kenyon, “Gunnery Tool Hits the Mark,” *SIGNAL Magazine*, March 2005, accessed November 12, 2016, <http://www.afcea.org/content/?q=gunnery-tool-hits-mark>.

without either VHF radio or SATCOM, but still at ranges beyond line-of-sight through the use of HF radio. This software improvement is now a common capability, and AFATDS might be the only mission command system with adequate redundancy in the event of a conventional war with counter-space and EW in full play. The Army should require vendors to provide software revision to allow all mission command systems to operate at lower data rates through CNR.

If more mission command systems are to operate via terrestrial CNR—and thus increase exposure to terrestrial EW jammers and sensors—the Army will need to improve CNR’s electronic protection, increase range, and data rates. To mitigate the threat of electronic sensing and jamming, the Army should increase fielding of directional antennas for terrestrial CNR, which would also improve transmission range and data rates. A RAND study on Army bandwidth requirements claims that using steerable directional antennas can increase data throughput “between 70 to 370 percent.”¹²² The same report also cited a negative correlation between beam-width and relative capacity improvement (see Figure 9). Some Ukrainian Army units are using parabolic dish antennas to increase range between units.¹²³ Harris® currently sells a log periodic directional antenna (see Figure 10) that is compatible with VHF CNR.¹²⁴ Fielding of directional antennas would provide higher data rates for mission command systems, would allow increased range, and would avoid the 360-degree exposure to jamming and direction finding.

¹²² Leland and Porche, *Future Army Bandwidth Needs and Capabilities*, 48.

¹²³ Joint Multinational Training Group-Ukraine et al., “Lessons Learned from the UKR 1-24th Mech BDE,” 15.

¹²⁴ Harris, *AN/PRC-117F(C) Multiband Multimission Radio Applications Handbook* (Harris, n.d.), 12.

Sender Beamwidth (degrees)	Receiver Beamwidth (degrees)	Relative Capacity Improvement
20	20	324
30	30	144
90	90	16
20	omni	18
30	omni	12
90	omni	4

Figure 9. Relative capacity improvement of directional antennas. Leland and Porche, *Future Army Bandwidth Needs and Capabilities*, 47.

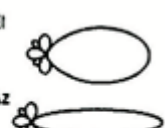
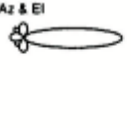
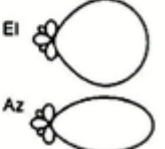
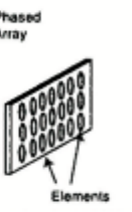
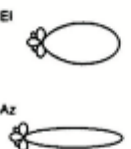
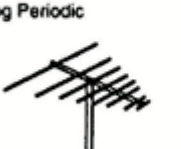
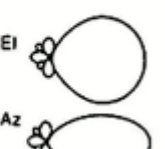
		Polarization: Linear Beamwidth: 40° x 40° Gain: 5 to 10 dB Bandwidth: 4 to 1 Frequency Range: VHF through mmw			Polarization: Depends on Feed Beamwidth: 5° to 30° Gain: 10 to 55 dB Bandwidth: Depends on Feed Frequency Range: UHF to μw
		Polarization: Horizontal Beamwidth: 90° x 50° Gain: 5 to 15 dB Bandwidth: 5% Frequency Range: VHF through UHF			Polarization: Depends on Elements Beamwidth: 5° to 30° Gain: 10 to 40 dB Bandwidth: Depends on Elements Frequency Range: VHF to μw
		Polarization: Vertical or Horizontal Beamwidth: 80° x 60° Gain: 6 to 8 dB Bandwidth: 10 to 1 Frequency Range: HF through μw			

Figure 10. Possible directional antennas for combat net radio with estimated horizontal (Az) and vertical (EI) beamwidths. Adapted from Adamy, *EW 103*, 58.

The Army should consider phased array antennas given their ability for rapid electronic steering to null out jamming signals and to narrow transmission beams between 5 and 30 degrees, while also increasing transmission range (See Figure 10).¹²⁵ Additional solutions may include “smart” antennas that expand and contract their beam based on the locations of friendly units. Such antennas could also have a mode that automatically adjusts the power amplification based on the

¹²⁵ Adamy, *EW 103*, 63–65.

required range. Such characteristics would optimize CNR performance while minimizing exposure to electronic sensors (see Figure 11).

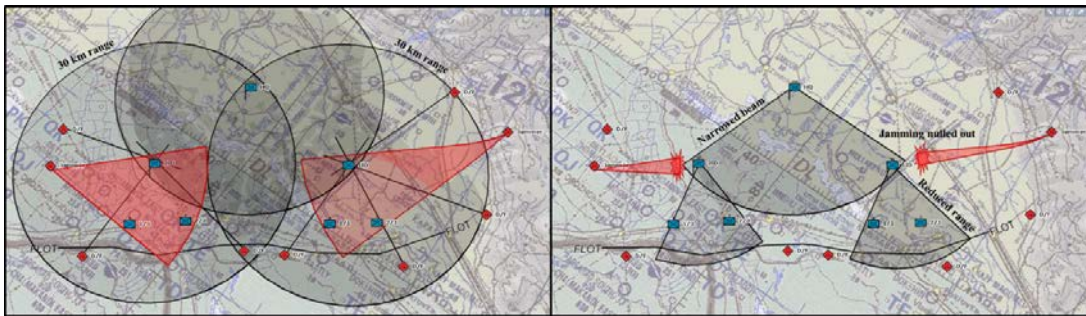


Figure 11. Comparison of omnidirectional antennas (left) with directional antennas (right). The omnidirectional antennas at full range maximize exposure to direction finders (D/Fs) and jammers. Directional antennas avoid these threats by adjusting beam-width and range based on the locations of friendly units. Created by the author using the National Geospatial-Intelligence Agency ONC “Base Background Map, 1:1,000,000.”

Some platforms will require mostly omnidirectional transmission, and for these the Army should field null steering processors to allow the proper balance of communications flexibility and electronic protection. A concept not yet fully researched is to develop adaptive antennas connected to *friendly* direction finders. These direction finders would provide a line of bearing for each friendly transmission. With the receipt of each friendly transmission, the directional antenna or steerable null processor could adjust so that the antenna sends and receives with a beam-width that includes only the relevant friendly units (see Figure 11). Such coupling of a receiver-transmitter with a direction finder would be especially useful when GPS receivers are jammed, allowing headquarters to know where their subordinates are each time they transmit.

Doctrine

Communications doctrine should put greater emphasis on ECCM, particularly the practice of emission control. The Signal Center of Excellence should be the proponent for ECCM so that there is no separation between the practice of effective communication and the masking of communication systems from electronic sensors and jammers. The two tasks should be completed in the same act. Communications doctrine should also stress the need for system redundancy, so that Army communication specialists understand that SATCOM is not a guaranteed enabler.

Maneuver and mission command doctrine cannot be separate from communications and electronic protection. Maneuver doctrine should include considerations for the movement and positioning of forces in a manner that masks their communication emissions from threat sensors, just as maneuver tactics and techniques prescribe methods for using terrain and vegetation to conceal movement from observation. Mission command doctrine should include discussion on the risks and benefits of decreased synchronization to allow a reduced communication electronic signature. Conveniently, the concept of mission command—with emphasis on decentralized operations and small-unit initiative—complements the practice of reduced communication. In combat, reducing communication with subordinate units comes with the small risk of losing some control. However, the practice of incessant radio traffic in the face of a growing EW threat carries a much higher risk: broadcasting friendly locations to enemy direction finders.

Training

Exercise rotations at the combat training centers (CTCs) of Ft. Irwin, Ft. Polk, and Hohenfels, Germany, should include periods of degraded and denied satellite connectivity. In addition to confirming the ability of mission command systems to function without SATCOM and through CNR mediums, the loss of SATCOM would force rotational units to revise their scheme of maneuver to make up for line-of-sight issues that SATCOM would have overcome. Such scenarios are likely in real combat against a peer adversary, and CTCs should be replicating the real fight with as much fidelity as practicable.

Routinely, units should practice various levels of emission control depending on the threat scenario. At times, the threat scenario should allow more liberal use of CNR. Other times, the EW threat should be escalated to encourage the use of directional antennas, radio silence, and terrain masking, while also forcing leaders and subordinates to understand the flexibility required to out-maneuver and out-smart EW attack and direction finding. Units should also practice communicating through field wire to account for situations when that is the only way to elude

enemy direction finders. Such situations would include the conduct of defensive tasks, screening, guarding, etc.

Conclusion

The United States Navy anticipated attritional tactics with night torpedo attacks by the Imperial Navy, but its leaders failed to follow up this insight with rigorous programs of material preparation and training to meet this clearly recognized threat. Too many officers ladled on top of this error a ‘fatal lethargy of mind’ as to the capabilities of the Imperial Navy.

—Richard B. Frank, *Guadalcanal*

US ground forces are significantly vulnerable due to a dangerous reliance on SATCOM and a lack of readiness to face a formidable counter-space and communications EW threat. Geographic limitations will reduce SATCOM availability in certain regions. SATCOM will remain vulnerable to increasingly effective counter-space technology. Consequently, current mission command systems will be of little use in such space-denied environments. In the likely event of SATCOM loss, the US Army will increase use of CNR, even though CNR will not allow most mission command systems to communicate. Uncontrolled and undisciplined use of CNR for lengthy orders transmission, incessant reporting, and constant centralized coordination will allow enemy sensors to quickly locate and destroy a slow, clumsy, and confused US ground force.

The US Army must not emulate the “lethargy of mind” to which the US Navy succumbed in the Pacific against the Japanese Imperial Navy. The Army has already *anticipated* an enemy counter-space and EW threat, now the Army simply needs to readjust its equipment, training, and doctrine to prepare for that threat. The US Army need not wait for a crisis to make this transition, but can instead develop a solution to the counter-space and EW threats before American troops face those challenges on an unforgiving field of battle.

Bibliography

- Adamy, David. *EW 103: Tactical Battlefield Communications Electronic Warfare*. Boston, MA: Artech House, 2009.
- Antal, John. "Simplify, Simplify, Simplify: An Update on the US Army's Lower Tactical Internet Effort." *Military Technology*, February 2015.
- Army Techniques Publication (ATP) 3-36, *Electronic Warfare Techniques*. Washington, DC: Government Printing Office, 2014.
- Army Techniques Publication (ATP) 6-02.72, *Multi-Service Tactics, Techniques, and Procedures for Tactical Radios*. Washington, DC: Government Printing Office, 2013.
- Baram, Abdul Karim. *Technology in Warfare: The Electronic Dimension*. Abu Dhabi, UAE: The Emirates Center for Strategic Studies and Research, 2008.
- Blair, David. "Russian Forces 'Practised Invasion of Norway, Finland, Denmark and Sweden,'" June 26, 2015. Accessed on November 12, 2016.
<http://www.telegraph.co.uk/news/worldnews/europe/russia/11702328/Russian-forces-practised-invasion-of-Norway-Finland-Denmark-and-Sweden.html>.
- Bolton, David. *The Challenge of Electronic Warfare*. London: Royal United Services Institute for Defence Studies, 1986.
- Buckhout, Laurie G. Moe. "Signal Security in the Ardennes Offensive: 1944-1945." US Army Command and General Staff College, 1997. Accessed on October 12, 2016.
<http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll2/id/829>.
- Byrne, Edward, and Paul Konyha, eds. *Space Primer*. Maxwell Air Force Base, AL: Air University Press, 2009.
- Carroll, John M. *Secrets of Electronic Espionage*. New York, NY: EP Dutton & Co., Inc., 1966.
- Chaplain, Cristina T. Space Acquisitions: Some Programs Have Overcome Past Problems, but Challenges and Uncertainty Remain for the Future, § Subcommittee on Strategic Forces, Committee on Armed Services (2015). Accessed on October 22, 2016.
<http://www.gao.gov/assets/670/669930.pdf>.
- Chapman, Bert. *Space Warfare and Defense: A Historical Encyclopedia and Research Guide*. Santa Barbara, CA: ABC-CLIO, 2008.
- Deakin, Richard S. *Battlespace Technologies: Network-Enabled Information Dominance*. Boston, MA: Artech House, 2010.
- Defense Science Board. "21st Century Military Operations in a Complex Electromagnetic Environment." Washington, DC, July 2015. Accessed on November 14, 2016.
http://www.acq.osd.mil/dsb/reports/DSB_SS13--EW_Study.pdf.
- Department of Defense. "Enhanced Polar System (EPS)." Selected Acquisition Report (SAR). Los Angeles, CA, March 18, 2015. Accessed on November 19, 2016.
http://www.dod.mil/pubs/foi/Reading_Room/Selected_Acquisition_Reports/16-F-0402_DOC_17_EPS_DEC_2015_SAR.pdf.
- Director, Operational Test and Evaluation. "FY 2015 Annual Report," January 2016.
- . "Warfighter Information Network-Tactical (WIN-T) Increment 2, Second Follow-on Operational Test and Evaluation," 2015.

- DishPointer. "Satellite Finder/Dish Alignment Calculator with Google Maps." Accessed on November 8, 2016. <http://www.dishpointer.com>.
- Donahue, Patrick J., and United States Army Forces Command. "Force Command Mission Command Network Priorities," April 26, 2016.
- Field Manual (FM) 3-38, *Cyber Electromagnetic Activities*. Washington, DC: Government Printing Office, 2014.
- Field Manual (FM) 3-55.93, *Long-Range Surveillance Unit Operations*. Washington, DC: Government Printing Office, 2009.
- Field Manual (FM) 6-02.72, *Tactical Radios*. Washington, DC: Government Printing Office, 2002.
- Field Manual (FM) 11-1, *Talk II-SINCGARS*. Washington, DC: Government Printing Office, 1996.
- Field Manual (FM) 11-45, *Signal Support to Theater Operations*. Washington, DC: Government Printing Office, 1999.
- Field Manual (FM) 24-18, *Tactical Single-Channel Radio Communication Techniques*. Washington, DC: Government Printing Office, 1987.
- Field Manual Interim (FMI) 6-02.45, *Signal Support to Theater Operations*. Washington, DC: Government Printing Office, 2007.
- Flynn, Michael T. Annual Threat Assessment, § Senate Armed Services Committee (2014). Accessed on November 25, 2016. http://www.dia.mil/Portals/27/Documents/News/2014_DIA_SFR_SASC_ATA_FINAL.pdf
- Frank, Richard B. *Guadalcanal: The Definitive Account of the Landmark Battle*. New York: Penguin Books, 1992.
- Frater, Michael R., and M. J. Ryan. *Electronic Warfare for the Digitized Battlefield*. The Artech House Information Warfare Library. Boston: Artech House, 2001.
- Freedberg, Sydney J. "Miserable, Disobedient & Victorious: Gen. Milley's Future US Soldier." *Breaking Defense*, October 5, 2016. Accessed on November 25, 2016. <http://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us-soldier/>.
- Freedberg Jr., Sydney J. "Army Radios Get Low Marks From DOTE." *Breaking Defense*, January 29, 2014. Accessed on November 25, 2016. <http://breakingdefense.com/2014/01/army-radios-get-low-marks-from-dote/>.
- Garden, Timothy. *The Technology Trap*. Exeter, United Kingdom: Brassey's Defence Publishers, 1989.
- Gertz, Bill. "Russia Conducts Fifth Test of New Anti-Satellite Missile." *Washington Free Beacon*. Accessed January 19, 2017. <http://freebeacon.com/national-security/russia-conducts-fifth-test-new-anti-satellite-missile/>.
- Grau, Lester W., and Charles K. Bartles. "The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces (Draft)." Ft. Leavenworth, KS: Foreign Military Studies Office, 2016.
- Greene, Harry, Larry Stotts, Ryan Paterson, and Janet Greenburg. "Command Post of the Future: Successful Transition of a Science and Technology Initiative to a Program of Record." *Defense Acquisition Research Journal* 17 no. 1, no. 53 (January 2010): 3–25.

- Harley, Jeffrey S. "Reading the Enemy's Mail: Origins and Development of US Army Tactical Radio Intelligence in World War II, European Theater of Operations." US Army Command and General Staff College, 1993.
- Harris. *AN/PRC-117F(C) Multiband Multimission Radio Applications Handbook*. Harris, n.d.
- Headquarters, 5th Army, US Army. "Outline Plan, Operation Shingle, Air Plan Communications," January 12, 1944. Accessed December 2, 2016. <http://cgsc.cdmhost.com/cdm/singleitem/collection/p4013coll8/id/3942/rec/1>.
- Headquarters, 6th Infantry Division, US Army. "Field Order 1, Annex XIII," November 28, 1944. Accessed December 2, 2016. <http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll8/id/29>.
- Headquarters, Eighth Army, US Army. "Field Order 17, Annex 5," January 22, 1945. Accessed December 2, 2016. <http://cgsc.cdmhost.com/cdm/singleitem/collection/p4013coll8/id/3064/rec/2>.
- Intelligence Science Board. "Integrated Sensor-Collected Intelligence." Washington, DC: Department of Defense, 2008.
- Joint Multinational Training Group-Ukraine, USAREUR Inspector General, USAREUR G2X, Center for Army Lessons Learned, Asymmetric Warfare Group, and 66th Theater Intelligence Brigade. "Lessons Learned from the UKR 1-24th Mech BDE." Yavoriv, Ukraine: International Peacekeeping Security Center, April 14, 2016.
- Kahn, David. *Hitler's Spies: German Military Intelligence in World War II*. New York: Macmillan, 1978.
- Karber, Phillip, and Joshua Thibeault. "Russia's New Generation Warfare." *The Potomac Foundation*, May 13, 2016. Accessed December 2, 2016. <http://www.thepotomacfoundation.org/russias-new-generation-warfare-2/>.
- Kenyon, Henry S. "Gunnery Tool Hits the Mark." *SIGNAL Magazine*, March 2005. Accessed November 12, 2016. <http://www.afcea.org/content/?q=gunnery-tool-hits-mark>.
- Klein, Christopher. "A Perfect Solar Superstorm: The 1859 Carrington Event." *History in the Headlines*, March 14, 2012. Accessed November 12, 2016. <http://www.history.com/news/a-perfect-solar-superstorm-the-1859-carrington-event>.
- Lamothe, Dan. "'We Will Pay the Butcher's Bill in Blood': General Issues Stern Warning as He Becomes Army Chief." *Washington Post*, August 14, 2015. <https://www.washingtonpost.com/news/checkpoint/wp/2015/08/14/we-will-pay-the-butchers-bill-in-blood-general-issues-stern-warning-as-he-becomes-army-chief-of-staff/>.
- Leland, Joe, and Isaac Porche. *Future Army Bandwidth Needs and Capabilities*. Santa Monica, CA: RAND, 2004.
- Lockheed Martin. "Lockheed Martin MUOS Satellite Tests Show Extensive Reach in Polar Communications Capability," January 31, 2014. <http://www.lockheedmartin.com/us/news/press-releases/2014/january/131-ss-muos.html>.
- Loverro, Douglas L. Statement of Mr. Douglas L. Loverro Deputy Assistant of Secretary of Defense for Space Policy, § Senate Committee on Armed Services Subcommittee on Strategic Forces (2014). http://www.armed-services.senate.gov/imo/media/doc/Loverro_03-12-14.pdf.
- McCaney, Kevin. "Army Still Catching Flak for Tactical Intell System." *Defense Systems*, March 22, 2016. <https://defensesystems.com/articles/2016/03/22/army-dcgs-a-criticism.aspx>.

- McCleary, Paul. "Russia's Winning the Electronic War." *Foreign Policy*, October 21, 2015. <https://foreignpolicy.com/2015/10/21/russia-winning-the-electronic-war/>.
- Moore, Charlie. "Russia Successfully Tests Anti-Satellite Missile." *Daily Mail*, May 27, 2016. <http://www.dailymail.co.uk/news/article-3612851/Russia-successfully-tests-anti-satellite-missile-capable-wiping-navigation-communications-intelligence-devices.html>.
- Nilson, Thomas. "Norway Creates New Army Unit on Border to Russia." *The Independent Barents Observer*, July 17, 2016. <http://thebarentsobserver.com/security/2016/06/norway-creates-new-army-unit-border-russia>.
- Office of the Secretary of Defense. "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2016." Washington, DC, 2016. Accessed on November 25, 2016. <http://www.defense.gov/Portals/1/Documents/pubs/2016%20China%20Military%20Power%20Report.pdf>.
- . "Annual Report to Congress: Military Power of the People's Republic of China 2006." Washington, DC, 2006. <http://www.dod.mil/pubs/pdfs/China%20Report%202006.pdf>.
- Organization for Security and Co-operation in Europe, Special Monitoring Mission to Ukraine. "Camouflaged 'R-330ZH Zhitel' Jamming Station." 2016.
- Payton, Matt. "Norway Is Now a Nuclear Target." *The Independent*, November 1, 2016. <http://www.independent.co.uk/news/world/europe/norway-nuclear-target-us-marines-russia-politician-weapons-a7390386.html>.
- Phillips, Tony. "Near Miss: The Solar Superstorm of July 2012." NASA, July 23, 2014. Accessed November 12, 2016. https://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm.
- Pillsbury, Michael. "China's Military Strategy toward the US: A View from Open Sources." Air University Press, 2001. Accessed November 2, 2016. <http://www.au.af.mil/au/awc/awcgate/china/strat.pdf>.
- Proesch, Roland. *Technical Handbook for Radio Monitoring VHF/UHF*. Germany: Books On Demand, 2013.
- Richardson, Doug. *An Illustrated Guide to the Techniques and Equipment of Electronic Warfare*. New York, NY: Arco Pub, 1985.
- Riley, Pete. "On the Probability of Occurrence of Extreme Spaceweather Events." *Space Weather* 10 (2012). Accessed November 13, 2016. <http://onlinelibrary.wiley.com/doi/10.1029/2011SW000734/epdf>.
- Rockwell, James M., ed. *Tactical C³ for the Ground Forces*. AFCEA/SIGNAL Magazine C³I Series, v. 4. Washington, DC: AFCEA International Press, 1986.
- Rood, Robert D. "FM Tactical Communications under Intentional Interference." US Army Command and General Staff College. Accessed October 4, 2016. <http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll2/id/1354>.
- Rose, Gideon. *How Wars End: Why We Always Fight the Last Battle*. New York, NY: Simon & Schuster, 2011.
- Shachtman, Noah. "Pentagon Paying China — Yes, China — To Carry Data." *Wired*. Accessed November 4, 2016. <https://www.wired.com/2013/04/china-pentagon-satellite/>.

- Simulation Interoperability Standards Organization EPLRS/SADL Product Development Group (PDG). "Enhanced Position Locating Reporting System (EPLRS)." Orlando, FL: Simulation Interoperability Standards Organization (SISO), Inc., 2013.
- Sterling, Christopher H., ed. *Military Communications: From Ancient Times to the 21st Century*. Santa Barbara, CA: ABC-CLIO, 2008.
- Thompson, Loren. "Electronic Warfare: How The U.S. Army Could Lose Its Next War." *Forbes*. Accessed October 19, 2016. <http://www.forbes.com/sites/lorenthompson/2016/03/15/electronic-warfare-how-the-u-s-army-could-lose-its-next-war/>.
- Thucydides, Robert B. Strassler, and Richard Crawley. *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*. New York, NY: Free Press, 2008.
- United States Government Accountability Office. "Defense Satellite Communications: DOD Needs Additional Information to Improve Procurements." Washington, DC, 2015.
- USCC. "2015 Report to Congress of the U.S.-China Economic and Security Review Commission," 2015. Accessed November 13, 2016. http://www.uscc.gov/Annual_Reports/2015-annual-report-congress.
- Vayavananda, Tatum. "Marine Corps Equipment Rolls out of Classified Norwegian Caves." *United States Marine Corps*, December 2, 2016. Accessed November 9, 2016. <http://www.marines.mil/News/News-Display/Article/655368/marine-corps-equipment-rolls-out-of-classified-norwegian-caves/>.
- Wen-Chi, Huang. "China's Space Capabilities and Their Regional Security Implications." US Army War College, 2011.
- Wilgenbusch, Ronald C., and Alan Heisig. "Command and Control Vulnerabilities to Communications Jamming." *Joint Forces Quarterly*, no. 69 (Quarter 2013): 56–63.
- Zell, Holly. "Impacts of Strong Solar Flares." NASA, June 7, 2013. Accessed November 9, 2016. http://www.nasa.gov/mission_pages/sunearth/news/flare-impacts.html.