
THE
LAND
WARFARE
PAPERS

No. 115 NOVEMBER 2017

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

Major Andrew H. Boyd

A National Security Affairs Paper
published on occasion by
THE INSTITUTE OF
LAND WARFARE
ASSOCIATION OF THE
UNITED STATES ARMY
Arlington, Virginia

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

by

**Major Andrew H. Boyd**

**The Institute of Land Warfare**
ASSOCIATION OF THE UNITED STATES ARMY

**AN INSTITUTE OF LAND WARFARE PAPER**

The purpose of the Institute of Land Warfare is to extend the educational work of AUSA by sponsoring scholarly publications, to include books, monographs and essays on key defense issues, as well as workshops and symposia. A work selected for publication as a Land Warfare Paper represents research by the author which, in the opinion of ILW's editorial board, will contribute to a better understanding of a particular defense or national security issue. Publication as an Institute of Land Warfare Paper does not indicate that the Association of the United States Army agrees with everything in the paper but does suggest that the Association believes the paper will stimulate the thinking of AUSA members and others concerned about important defense issues.

**LAND WARFARE PAPER No. 115, November 2017**

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

by Major Andrew H. Boyd, U.S. Army

Major Andrew H. Boyd is currently an officer assigned to the First Armored Division, Fort Bliss, Texas. He is a graduate of the U.S. Army Command and General Staff School, Fort Leavenworth, Kansas, and holds Masters degrees from the University of Oklahoma and the U.S. Army Advanced Military Studies Program. His previous assignments include command and staff positions in the 3rd Infantry Division, 4th Infantry Division and the Joint Multinational Readiness Center, Hohenfels, Germany.



Inquiries regarding this and future Land Warfare Papers should be directed to: Director, AUSA's Institute of Land Warfare, 2425 Wilson Boulevard, Arlington VA 22201, e-mail *ncurry@ausa.org* or telephone (direct dial) 703-907-2636 or (toll free) 1-800-336-4570, ext. 2636.

# Contents

# Acronyms

| | |
|---|---|
| AEHF | Advanced Extremely High Frequency |
| AFATDS | Advanced Field Artillery Tactical Data System |
| AFRICOM | United States 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 |
| FM | Field Manual |
| 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 |
| Kbps | Kilobits per second |
| Km | Kilometer |

| | |
|---|---|
| LAN | Local Area Network |
| LEO | Low-earth Orbit |
| Mbps | Megabits per second |
| MCPP-N | Marine Corps Prepositioning Program-Norway |
| MNVR | Mid-tier Networking Vehicular Radio |
| MUOS | Mobile User Objective System |
| NATO | North Atlantic Treaty Organization |
| 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 | United States–China Economic and Security Review Commission |
| VHF | Very-high Frequency |
| WIN-T | Warfighter Information Network-Tactical |

# Preface

Threats to communication satellites and ground communication systems will present significant challenges to the U.S. Army in a conventional war. The Army is significantly dependent on satellite communication (SATCOM) 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' counterspace capabilities can disrupt the Army's access to SATCOM and U.S. forces operating at northern extremes may not have connection due to geosynchronous satellite geometry. This would leave U.S. forces more reliant on their terrestrial communication systems. Although the U.S. 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 could target U.S. communication systems. Given the threats to satellite and ground communication systems, the U.S. Army is unlikely to be successful in a conventional war against a comparable adversary without significant change to equipment, doctrine and training.

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

*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. . . . [C]onstant 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, *The Landmark Thucydides*[1]

## Introduction

United States ground forces are and will be significantly vulnerable in present and future conflicts due to a dangerous reliance on satellite communication (SATCOM) and a degraded 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 liabilities for which the U.S. 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 U.S. military's overall technological lead over near-peer threats has narrowed, the U.S. 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 that they need to communicate and fight effectively in an environment where both space and the electromagnetic spectrum are contested.

One of the U.S. 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 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 U.S. military to channel its operational communications through the leased networks of commercial satellites; these 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 U.S. dependence on SATCOM. They have developed

formidable capabilities—such as jamming and anti-satellite missiles—to attack that dependence. Even without human threats to SATCOM, periodic geomagnetic storms can damage satellites in orbit. Besides these challenges, most communication satellites do not function north of 65°N latitude; this area includes zones for potential conflict with Russia. Despite these concerns, most ground force communications are structured to require consistent SATCOM.

As the U.S. Army's celestial communication systems have enjoyed an apparent sanctuary in space, terrestrial communications EW has been put on the back burner. Advances in U.S. electronic counter-countermeasures (ECCM), the fall of the Soviet Union and the low EW threat in the conflicts in Iraq and Afghanistan have all contributed to the Army's apathy toward communications protection. Current doctrinal manuals that describe communication practices and EW often lack the depth and tactical solutions that Cold War doctrine once provided to combat the EW threat. The decision to field ground communication systems with highly-detectable electromagnetic signatures points to an Army doctrine and culture that does not place enough emphasis on terrestrial communications EW threats.

To overcome these significant vulnerabilities, the U.S. Army must procure communication systems that maintain the information high ground, but also allow redundancy, flexibility and survivability against threats. The Army must also refine its doctrine to place proper emphasis on the possibility of electronic attack and detection. Individual and collective training should combine the right equipment and techniques to ensure that units are training for a realistic fight—one that would include periods of denied SATCOM and an increased risk 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."[2] A key element of remaining strong on the ground is maintaining the capability to communicate effectively 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, but its capabilities will be severely degraded. The Army's leaders and Soldiers can adapt—but the equipment, training and doctrine of today will determine how steep that learning curve of adaptability will be and what price in blood the U.S. Army will pay for it. Current communication vulnerabilities will face increasingly complex and sophisticated threats; the benefit of prescient groundwork in peace is preferable to costly improvisation in a time of war.

**Satellite Communication: U.S. Army's Dependence**

SATCOM is a critical component of tactical ground force communication structure. It 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.[3] High Frequency (HF) radios can transmit voice and data over thousands of kilometers through ionospheric refraction (by bouncing off the ionosphere); data rates, however, are limited to 9.6 Kbps,[4] which is insufficient for most mission command systems. Volatile ionospheric conditions can also 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 that is roughly 47 square km.[5] 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,[6] 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, proximity to the equator allows SATCOM to function without terrain or man-made structures that frequently block connections between ground terminals and satellites. SATCOM also provides data rates that are much higher than the 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.[7] SATCOM ground terminals are also more resistant to terrestrial EW attack and interception than most combat net radios (CNR). Ground terminals connect with communication satellites by pointing directional antennae 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 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 U.S. Army has leveraged that capability and so increased its reliance on SATCOM. During the Gulf War, up to 60 satellites supported the transfer of operational data, allowing U.S. ground units beyond the range of CNR to keep pace with rapid developments on the battlefield.[8] The amount of digital information that was communicated during the Gulf War "gave the war a new dimension" and paved the way for the further proliferation of military SATCOM;[9] dependence on bandwidth increased thirtyfold in the 13 years between Operation Desert Storm and Operation Iraqi Freedom.[10] Over the past 15 years, SATCOM-enabled Blue Force Tracking (BFT) has slowly eclipsed the terrestrial EPLRS as the primary communication medium for Force XXI Battle Command Brigade and Below. By 2017, the U.S. Army will completely divest EPLRS.[11, 12] A 2004 RAND study argues that terrestrial line-of-sight radio will not be sufficient to meet U.S. Army data needs and that SATCOM will continue to become even more crucial for Army operations.[13] An Intelligence Science Board report predicts that by 2020, total demand for SATCOM bandwidth will increase from 40 gigabits per second (Gbps) today to 80 Gbps by 2022; projected SATCOM coverage will only be capable of providing up to 50 Gbps, leaving a significant gap between supply and demand.[14]

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,[15] 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,[16] but this rate is beyond the capabilities of the terrestrial radio systems (SINCGARS, HF, EPLRS) discussed above. Although the AFATDS has the ability 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.

**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*[17]

> *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*[18]

*SATCOM Limitations*

Dependence on SATCOM comes with an array of geographic limitations and terrain interference. Most significant is the geographic limitation of the satellite capability to between 65°N and 65°S—it is only within this area that ground terminals and satellites can connect with each other.[19] Some may not consider this a significant concern for U.S. ground forces, given the geographic extremity of these polar regions. However, recent tension between the North Atlantic Treaty Organization (NATO) and Russia make conflict on the Scandinavian Peninsula and the Aleutian Islands of Alaska plausible. U.S. forces should be prepared to fight beyond 65°N in this region, but SATCOM is not a dependable form of communication for this area.

Half of Norway also lies north of 65°N latitude. This key NATO ally shares a 120-mile border with Russia; Russia 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 showed otherwise. In this exercise scenario, Russia simulated the invasion of these states in order to control access to the Baltic Sea, denying NATO the ability to reinforce its allies in Eastern Europe.[20] In response to a 2016 deployment of 330 U.S. Marines to a Norwegian airfield, a Russian defense official warned that Norway would now be on Russia's nuclear target list.[21] Norway takes the threat of Russian aggression seriously; it has fielded a new unit to patrol its border with Russia. This unit—more than a simple border and customs enforcement—is armed with anti-armor and anti-aircraft capabilities, both of which serve to deter and disrupt a possible Russian ground invasion.[22]

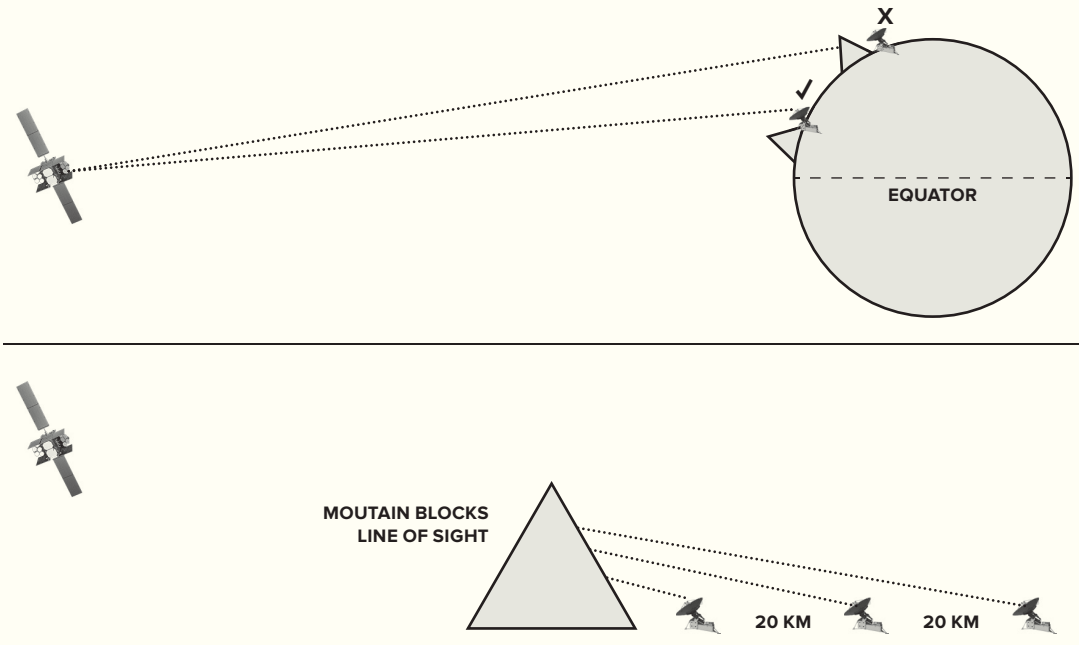
As part of a plan to ensure that NATO members can defeat territorial incursions, the United States Marine Corps maintains significant prepositioned materiel in Norway. The Marine Corps Prepositioning Program-Norway (MCPP-N) has a fleet of combat and support vehicles inside man-made caves that can facilitate the equipping of a Marine expeditionary brigade for operations in support of NATO allies.[23] Given NATO's preparation and Russia's rhetoric, conflict in northern Europe is plausible. In such a conflict, U.S. forces could easily find themselves fighting and attempting to communicate 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 farther from the equator. Because most military communication satellites orbit above the equator, these satellites will appear in the southern sky when observed

from the Northern Hemisphere. As an observer in the Northern Hemisphere moves farther north, the communication satellite will appear lower in the sky. In relatively flat and open terrain, this is not an issue. However, if a ground terminal has elevated terrain or infrastructure to its south, it may not be able to communicate with the desired satellite because of geographic interference. 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 little use to U.S. ground forces operating in mountainous terrain near these northern extremes.

*Figure 1*

## Terrain Effects on SATCOM

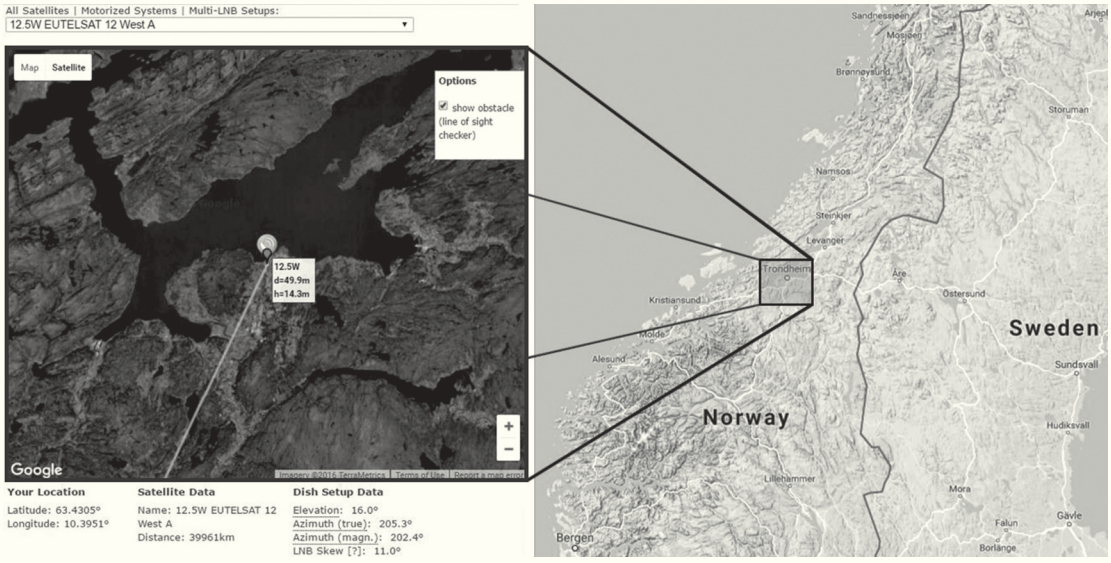



Although the ground terminals are within terrestrial range of each other, most of their mission command systems cannot communicate in such a situation when SATCOM is lost.

If U.S. ground forces were to operate with NATO forces to counter Russian aggression on the Scandinavian Peninsula and other northern locations, 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°N latitude. Although this is technically within most SATCOM footprints, it is 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 website that allows users to determine the azimuth and elevation to which they must orient their ground terminals in order to successfully connect to a satellite—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 50 meters away and only 15 meters high would obstruct the satellite signal.[24] 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 to achieve connectivity with the Eutelsat 12




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

As movement and fighting through Norway would continue, the steep terrain lining many of Norway's main roads would likely prevent reliable SATCOM. As maneuver units approach latitudes closer to 65°N, SATCOM terminals would have to lie exposed in open terrain in order to allow mission command systems to function. 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 with little or no cover. Maneuver decisions would have to be subordinate to communication limitations. For U.S. forces conducting potential operations at such northern extremes, SATCOM becomes more of a liability than an enabler. This raises questions about the ability of the U.S. 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.[25] The most recent testing of MUOS identified "200 high-priority hardware and software problems."[26] 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.[27] 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 and, 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.[28]

*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.[29] Potential adversaries such as Russia and China have attained the capability to exploit U.S. space dependence through jamming and anti-satellite (ASAT) missiles. The hazard of threat capabilities is exacerbated by the U.S. military's preponderant use of commercial communication satellites that are more vulnerable to jamming and cyber interference than military satellites. Even if U.S. forces are operating in the optimal geographic area for successful satellite connectivity, 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."[30] A repeat of the Carrington Event on today's digitized planet almost occurred on 23 July 2012; a solar storm crossed the earth's orbital path, missing the planet by about a week.[31] In *Space Weather*, Pete Riley predicts that there is a 12 percent chance of another CME hitting the earth in the next decade with the same magnitude as the Carrington Event.[32] 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.[33] 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 U.S. 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.

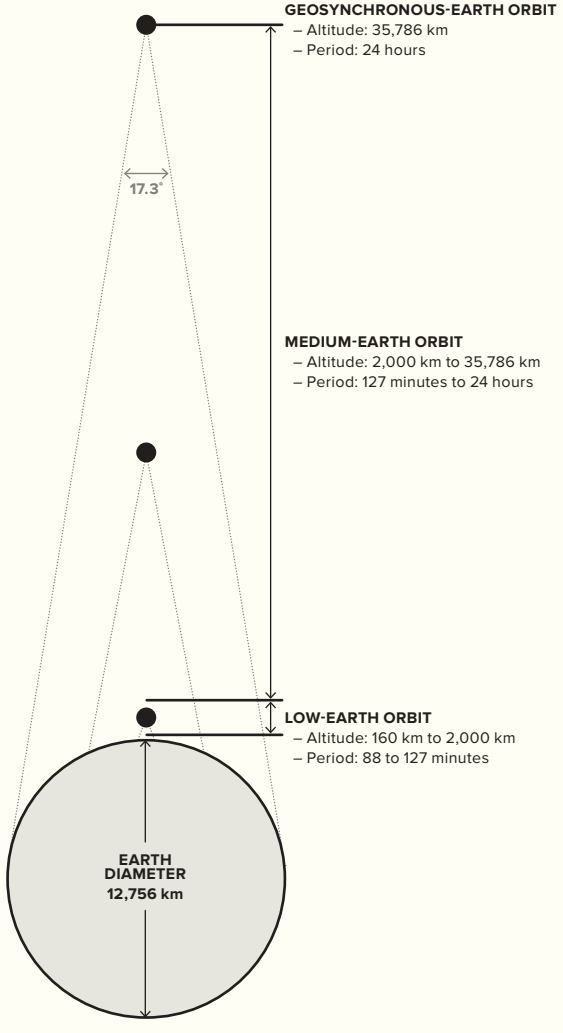
While unavoidable CMEs are a concern, intentional human interference with SATCOM is a more pressing matter. The People's Liberation Army (PLA) of China recognizes "the United State's high reliance on military space systems as a potential 'Achilles heel,'"[34] and has been researching and developing counterspace and ASAT capabilities since the 1960s.[35] 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."[36] Several Chinese universities have developed models for "space intercept control and terminal guidance systems"[37] to facilitate potential satellite attacks. At the strategic level, China's political and military elite clearly believe in the "inevitability of space militarization" and are developing capabilities to challenge U.S. access to space.[38]

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.[39] This event only proved China's capability to destroy satellites in low-earth orbit, such as imaging satellites. It did not necessarily prove China's capability to destroy communications satellites in geosynchronous-earth orbit (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,"[40] allowing the targeting of communications satellites. Such efforts have caused concern in the U.S. intelligence community that China's counterspace

capabilities "could destroy or disable U.S. satellites responsible for handling nearly 90 percent of U.S. military communications."[41] 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,"[42] causing the destruction of a cluster of satellites at a specific longitude. The strategic advantage of using a nuclear weapon in space against communication 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 U.S. SATCOM would likely not result in nuclear retaliation and mutually assured destruction, but would nonetheless have devastating effects on the United States and its allies.

*Figure 3*

## Satellite Orbits, Periods and Footprints




"Satellite Technology Challenges," Electropaedia, accessed 29 November 2016, http://www.mpoweruk.com/satellites.

The PLA continues to pursue the development of directed energy weapons to augment its ASAT capability. A 2015 report by the United States–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."[43] 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.[44] A Defense Intelligence Agency (DIA) report also confirmed that China has satellite jammers in development as well as other non-kinetic counterspace capabilities.[45]

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:[46]

> 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 anti-satellite 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.[47]

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.[48]

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

Russia has been historically competitive with the United States in counterspace development. Between 1968 and 1971, Russia conducted seven ASAT tests, five of which successfully destroyed satellites at altitudes of 230 to 1,000 km.[49] In a 2015 statement to the Senate Armed Services Committee, DIA director Lieutenant General Vincent R. Stewart warned that "Russian leaders openly assert that the Russian armed forces have antisatellite weapons and conduct antisatellite research." Russia proved its capabilities in May 2016 by launching the *Nudol* direct ascent missile that is capable of destroying communication satellites.[50] Russia tested this capability again in December of 2016 with its third successful launch of the *Nudol* from a base in central Russia.[51] Like the PLA, Russia also possesses the non-kinetic option to jam communication satellites.[52]

Commercial satellites augment military communication satellites by providing flexibility to U.S. forces operating in austere environments with little or 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 such a practical option that up to 90 percent of military satellite communication is through commercial vendors.[53] In 2011, the DoD spent over $1 billion on commercial SATCOM services.[54]

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 United States Africa Command (AFRICOM).[55] Use of communications satellites from companies that are controlled by potentially belligerent governments leaves the United States communications network vulnerable to monitoring and disruption. Also, because the data going through non-U.S. satellites is encrypted, prolonged exposure of such sensitive communications could provide Chinese intelligence agents valuable insight into U.S. military encryption technology.[56] Besides the threat of a state or private company intentionally meddling in U.S. military communication traffic, state neutrality in a time of war may prevent some SATCOM vendors from providing the commercial bandwidth upon which U.S. troops so heavily rely, thus disrupting force projection and operational tempo.

*Lack of SATCOM Redundancy*

Given potential adversaries' capabilities 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 the military's AEHF constellation;[57] their Wideband Global SATCOM system currently consists of six satellites in orbit.[58] Although there are over a thousand functioning satellites orbiting the earth, only a limited number are communications satellites. Of those, only so many can provide both sufficient bandwidth and orbit at the appropriate longitudinal position to provide redundancy in the event that 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.[59] Likewise, military communication satellites are not all interchangeable with regard to bandwidth capacity and orbital position.

If even a single U.S. communication satellite were destroyed, it could have devastating effects on communication for land forces.[60] Because a single AEHF satellite can support up to 6,000 terminals, 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.[61] Ground units would continue to lack communication either until they switched to a redundant satellite (if available), until they adopted a terrestrial CNR solution or until the U.S. could 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 originally scheduled launch date. In addition to the often lengthy emplacement time, satellites are expensive. The total AEHF program cost is currently at $14.6 billion, which is twice the original cost estimate.[62] The United States' acute reliance on communication satellites in war could mean significant replacement costs in time and money. This liability during a resource-constrained war could paralyze U.S. communication abilities and so facilitate the swift defeat of U.S. forces. The U.S. Army does recognize this dependence and is developing and fielding capabilities 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 data rates. Unfortunately, the most recent Follow-on Operational Test and Evaluation 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 percent 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 Fort Campbell, Kentucky.[63]

MNVR is capable of providing terrestrial communication for the Joint Battle Command–Platform that is primarily driven by SATCOM. However, an evaluation in 2013 determined that the MNVR was "not operationally suitable due to poor reliability."[64] During testing in 2015, MNVR was not capable of sending messages at distances as short as six to 10 km. In degraded SATCOM environments, it did not meet the message completion requirement of "90 percent at-the-halt and 85 percent on-the-move."[65] Even though the U.S. Army is making efforts to build terrestrial redundancy in the event of SATCOM loss, it is unlikely that it will fix SATCOM dependence in the near future.

Overreliance on SATCOM will undeniably pose some of the above challenges to an army at war. To fight effectively, U.S. ground forces must have mission command systems that can function through media other than SATCOM. Although many consider SATCOM critical to U.S. operations, it may be significantly degraded or eliminated to the point that commanders *must* rely on terrestrial communications. To continue the fight, U.S. forces will have to rely increasingly on terrestrial CNR—and that 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 to corps-level headquarters—will likely increase their use of terrestrial CNR. A corresponding increase in electronic signatures will raise their exposure to terrestrial EW threats. The U.S. Army has a strong historical and doctrinal precedent for countering these threats. Unfortunately, potential adversaries of the U.S. have increased their ability to target terrestrial CNR through direction finding and electronic countermeasures (ECM) such as jamming.[66] Meanwhile, the U.S. Army's confidence in its terrestrial systems' survivability against EW has allowed U.S. ground forces to become complacent and to develop communication practices that lack proper emphasis on countering these threats through ECCM.[67] 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.

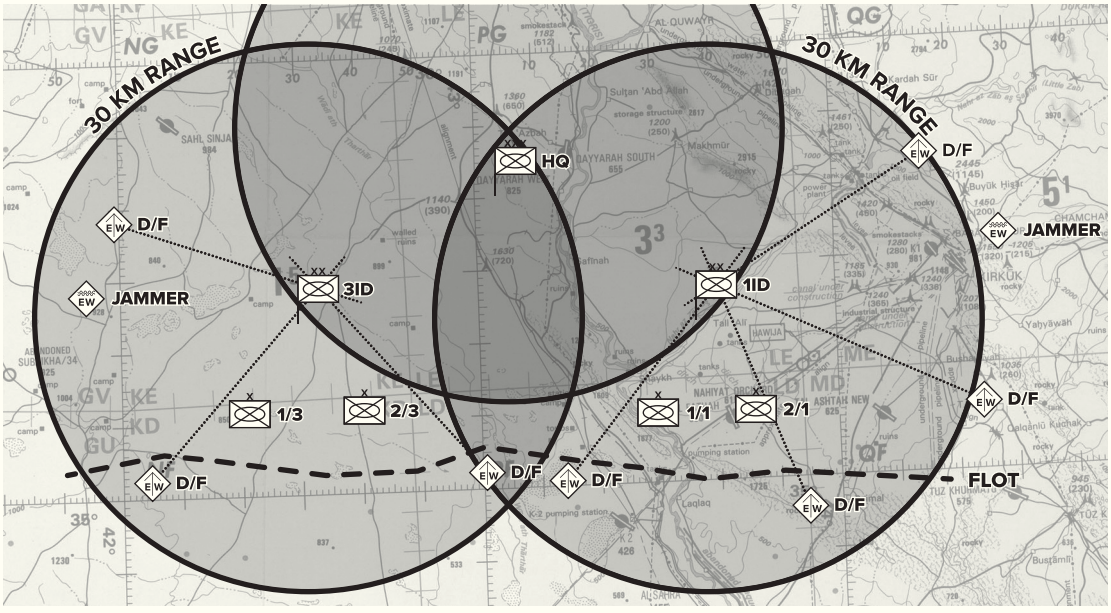
*A Precedent for Emission Control*

Both jamming and direction finding are significant concerns for ground force communication. Jamming is dangerous in that it prevents units from communicating, but it does not reveal units' positions to the enemy. Direction finding, however, is significantly more dangerous; even the most rapid transmission can allow the enemy to pinpoint units' locations and then attack them 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 km of the front line, they can normally attain a fix on the emitter with a 90 percent circular error probable (CEP) of 1,500 meters.[68] Today, some Russian direction finders have a direction of arrival (DOA) accuracy of one degree.[69] With this level of accuracy, two Russian direction finders could locate a friendly emitter 20 km away with a 500 meter 90 percent CEP. If they were 10 km away, the 90 percent CEP would be 170 meters.[70] Most enemy forces will fire on a 90 percent CEP if they have sufficient artillery.[71] 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.[72] 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

*Figure 4*

## Notional direction finding of division command posts

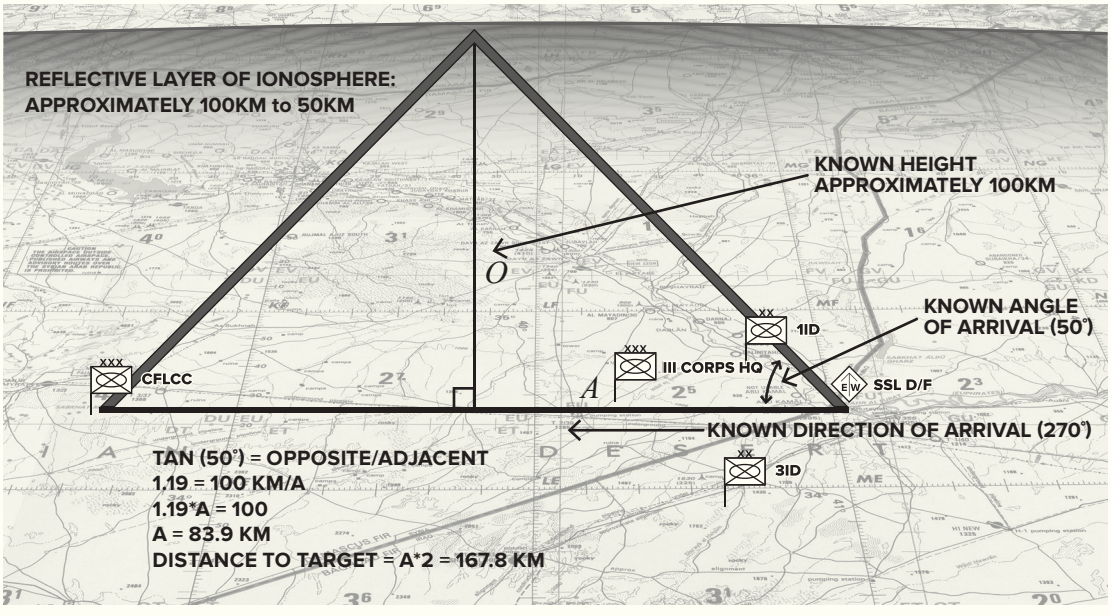



Enemy direction finders (D/Fs) acquire fixes on friendly command posts that are emitting at maximum range and in all directions.

*Created by the author using the National Geospatial-Intelligence Agency "Operational Navigation Chart G-4, 1:1,000,000."*

*Figure 5*

## Notional single-site location (SSL)




*Created by the author using the National Geospatial-Intelligence Agency "Operational Navigation Chart G-4, 1:1,000,000."*

location of the emitter, at which 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 U.S. 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, exercising 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.[73] The French also made use of direction finding in World War I; they were successful enough to "develop the [German] order of battle, track their forces as they moved, and determine their intent," allowing the French army to halt the Germans at the Battle of the Marne.[74]

When the American Expeditionary Force entered the war, their radio intelligence sections used direction finding to discern the German order of battle through traffic analysis.[75] The U.S. Army continued to employ direction finding during World War II, and army-level fronts in the European Theater of Operations often employed up to 12 direction finding stations on a 35-mile front.[76] Emission control is the most basic method to avoid threat direction finding. Emission control is achieved when transmissions are reduced to short "chirps," when the power and direction of transmissions are reduced, or when radio silence is broadly enforced.[77] 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 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 record the transmission and then slow it down for "normal listening."[78]

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 their consequential defeat at Tannenberg, the Russians enforced strict emission control to deny the Germans the opportunity to triangulate Russian positions.[79]

The U.S. 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 after the surprise element was completely lost—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 that limited reception by distant enemy sensors.[80] 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."[81] 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.[82]

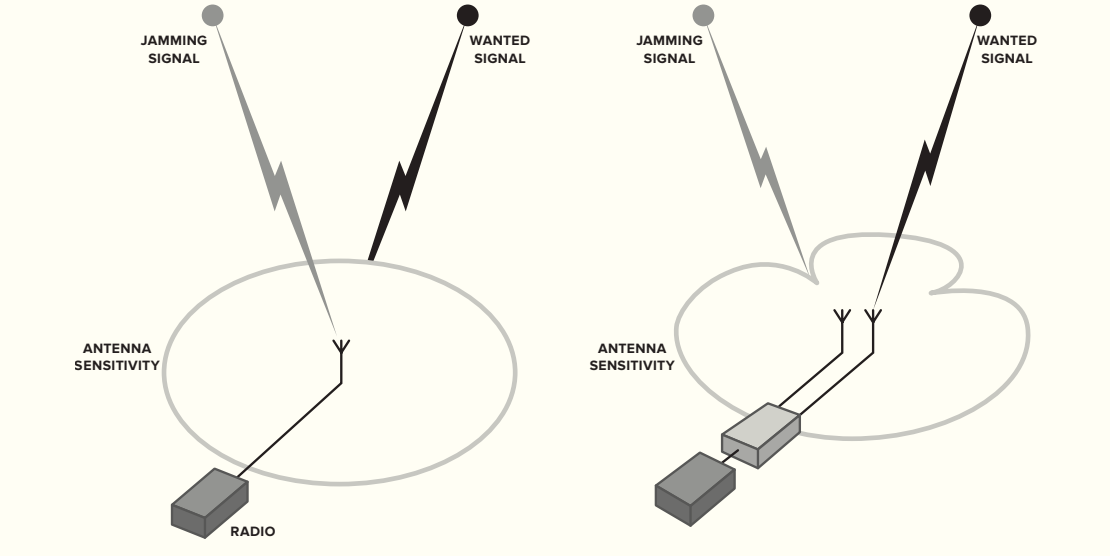
One way around such strict use of radio silence (and pigeons) was the Army's increased use of directional antennae. If a headquarters knows the general direction of the receiving friendly radio station, it can point a directional antenna in that general direction, instead of emitting a signature in all directions; naturally, this would limit their exposure to an enemy's sensors. Units on the front line can focus their antennae toward their parent headquarters, and parent headquarters can focus their antennae 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 antennae would provide additional range while avoiding enemy EW assets.[83] At the time of that writing, the U.S. Army took communications EW seriously enough that it developed a standardized directional log period antenna to mitigate these threats.[84] FM 24-18 described the science of radio theory in detail, providing an entire chapter on how to effectively communicate in the presence of EW threats and putting a strong emphasis on the use of directional antennae to avoid enemy jamming and to elude enemy direction finding.[85]

Another method the Army developed during the Cold War to avoid enemy EW assets was null steering. The Steerable Null Antenna Processor (SNAP-1), fielded in the 1980s, manipulated the frequencies of two antennae from the same radio to cancel out signals in the direction of an enemy jammer.[86] In addition to avoiding unwanted jamming signals, the friendly radio site could also "null out" the signal in the direction of suspected enemy direction finders, denying them a line of bearing.[87] The use of null steering provided a significant benefit because it maintained simplicity with 360° 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 the SINCGARS' frequency-hopping mode.[88]

Another system used in the 1980s was the Plessey Interference Cancellation Equipment (ICE; see Figure 6), which operated on the same principle. Through the ICE, the radio could

*Figure 6*

Plessy Interference Cancellation System




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

reduce "sensitivity in the direction of the jammer" and increase "reception of the wanted signal."[89] 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 used in U.S. Army communications ECCM.

Historical, doctrinal and technological precedent shows that the U.S. Army had a healthy concern for a defensive electronic posture during the Cold War. In this context, the U.S. Army continued to pursue technological improvement in electronic protection. The U.S. military began designing SINCGARS in 1974, with production deliveries starting in 1988.[90] SINCGARS replaced many of the Vietnam-era radios that were considerably more 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.[91]

Older enemy direction finders and jammers that are mechanically tuned cannot keep up with the automated speed of such ECCM.[92] Coinciding with the use of SINCGARS, the Army began fielding EPLRS in 1987.[93] EPLRS uses frequency-hopping and time division multiple access,[94] whereby each EPLRS radio "chirps" its positioning and messaging data in an allotted timeframe of 1.95 milliseconds,[95] thereby remaining quite elusive to electronic sensors. These developments gave the U.S. Army an edge of confidence in ECCM technology.

*Apathy Toward a Renewed Electronic Warfare Threat*

Advances in ECCM technology in the 1980s and the decline of the Soviet Union allowed the U.S. 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 U.S.-led coalition found it difficult to maintain radio discipline.[96] Despite inferior emission control, the coalition's overwhelming force prevailed, and the Iraqi Army quickly retreated from Kuwait. Following the U.S. Army's impressive performance in the Gulf War, the Soviet Union collapsed. With this significant reduction of competition, U.S. 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.[97] With the end of the Cold War, the U.S. military went through what would later be called "twenty-five years of EW neglect."[98]

A comparison of doctrine from the 1980s with today's doctrine shows the clear disparity in emphasis on electronic protection. In 1987, FM 24-18 devoted an entire chapter to an adversary's intentions and capabilities that threatened friendly communication. Eight pages focused solely on 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 17 times. It provides an entire appendix that describes the use of the SNAP-1. It explains in detail the inherent advantage of additional gain and avoidance of enemy jammers and direction finders.[99]

More recent doctrine does not share such an emphasis on the EW threat. Army Techniques Publication (ATP) 6-02.72, *Tactical Radios*, discusses ECCM only three times, directional antennae once and null steering not at all.[100] FM 6-02, *Signal Support to Operations*, does not mention directional antennae, 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 and ECCM are completely omitted.[101] In Field Manual Interim 6-02.45, *Signal Support to Theater Operations*, EW is mentioned three times and emission control only once.[102] After years of confidence in technological superiority and minimal EW threats to the U.S. Army, the current doctrine clearly does not adequately address renewed threats to communication systems.

While some people in the signal community might consider ECCM to be less in the purview of communications doctrine and more in the realm of EW doctrine, EW manuals are no better than communications manuals at covering ECCM. For example, FM 3-38, *Cyber Electromagnetic Activities*, which broadly discusses aspects of both cyber and EW, mentions emission control twice but does not specifically reference ECCM at all. The manual brings up directional antennae and other forms of ECCM only in passing:

> Take appropriate actions to minimize the vulnerability of friendly receivers to enemy jamming (such as reduced power, brevity of transmissions, and directional antennae). Ensure redundancy in all systems is maintained and personnel are well-versed in switching between systems.[103]

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 solutions for avoiding that type of detection. To be fair, ATP 3-36 does at least provide a definition for "electronic masking":

> …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.[104]

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 communications and EW doctrine indicates that the Army is not actively concerned with 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 is due to what was 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."[105] While SINCGARS can elude more primitive electronic sensors, today's computer-assisted jammers and direction finders can ascertain the pattern of frequency-hopping radios. With these advances in EW technology, frequency-hopping radios now stand out due to their emission of unique and sporadic "frequencies at a single location."[106] 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.[107] Frequency-hopping radios still have an advantage over analog EW equipment,

but the improvements in EW technology have made them easier (instead of more difficult) to identify when surrounded by non-military transmissions in single frequency.

The U.S. Army treats EW as an afterthought—more of an impediment to operations than an enabler.[108] However, the Russian military gives EW high priority.[109] **Today, each Russian maneuver brigade has its own EW company, while U.S. battalions will have only two EW personnel.**[110] Russia has sophisticated communication EW systems such as the R-330B very-high frequency (VHF) jamming and direction-finding system (see Figure 7) that 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 three degrees of accuracy, and it has a detection-to-suppression time of less than five milliseconds.[111] In a situation where access to SATCOM is denied, use of VHF for data and voice traffic will likely rise, leaving U.S. forces vulnerable to detection and triangulation with such systems as the R-330B.

*Figure 7*

R-330B Direction Finder

*Lester W. Grau and Charles K. Bartels, "The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces" (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), p. 244.*

Another notable Russian EW system is the R-378AM. This system can jam and find the direction of HF radio systems (see Figure 8), putting long-range transmitters at risk of being located through single-site location.[112] The Organization for Security Cooperation in Europe has identified similar EW systems employed in eastern Ukraine in support of pro-Russian separatists.[113] The use of such EW capabilities has caused considerable communication problems for Ukrainian forces, who consequently have to sometimes rely on hard-wired field telephones due to the frequency of Russian jamming[114] that often leaves their cell phones and radios "unusable for hours at a time."[115] The Russians pose an undeniable EW threat that the U.S. Army must address.

*Figure 8*

R-378AM Direction Finder and Jammer

*Lester W. Grau and Charles K. Bartels, "The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces" (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), p. 243.*

This lack of emphasis on communications EW coincides with the proliferation of precision-guided weaponry and unmanned aerial vehicles (UAVs) in the hands of U.S. adversaries. Potential adversaries today have precision capability that can completely destroy headquarters and massed forces at any echelon if their location is discovered. Even the slightest chirp of a radio emission picked up by a single direction finder can cue an enemy UAV, 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.[116]

This is one of many examples that have deeply resonated with military leaders in the United States as a caution to prepare for a fight with a near-peer adversary—a fight where there is no guarantee of technological superiority as there was in the Gulf War and in the 2003 invasion of Iraq. One U.S. 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."[117] General Milley described a future enemy with "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."[118]

**With an enemy constantly searching for signs of U.S. forces on the electromagnetic spectrum, one would think that the U.S. Army would not be likely to cultivate a doctrine that is naïve about electronic detection while simultaneously 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."[119] 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 U.S. forces. Although such networks are intended to allow information superiority, they come at the high risk of increasing the exposure of 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."[120]

While increasing the vulnerability of U.S. 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 Radio System waveform."[121] The HNW in particular did not function at line-of-sight ranges much longer than 10 km in the open desert of White Sands Missile Range, New Mexico. In the forested terrain of Fort Campbell, Kentucky, HNW functioned up to 2.5 km, but usually lost connectivity at 1 km.[122] 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 U.S. Army is "committed to using networking waveforms."[123] The fielding of such communication 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 U.S. formations to threat sensors.

The U.S. Army is significantly vulnerable to terrestrial EW attack and detection. Although there is strong historical, technological and doctrinal precedent for the 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 U.S. enjoyed in past conflicts will not continue against such a threat. The U.S. Army must address its EW capability gap.

**Recommendations**

The U.S. Army should prepare for the loss of SATCOM in a future conflict—such a loss is 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 U.S. Army is also likely to encounter significant terrestrial EW reconnaissance and attack. To address this threat, the Army should make immediate changes to equipment, doctrine and training.

*Equipment*

To equip for a future conflict with a persistent space and an EW threat, **the Army should divest WIN-T**. 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; in such a scenario, its network will also be dangerously visible to threat electronic sensors. 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 that 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 to the unit within two weeks.[124] This allowed AFATDS to function 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; AFATDS might be the only mission command system equipped with adequate redundancy in the event of a conventional war with counterspace and EW in full play. The Army should require vendors to provide software revision that would 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 and increase range and data rates. To mitigate the threat of electronic sensing and jamming, the Army should increase fielding of directional antennae for terrestrial CNR—this would also improve transmission range and data rates. A RAND study on Army bandwidth requirements claims that using steerable directional antennae can increase data throughput "between 70 to 370 percent."[125] The same report also cited a negative correlation between beam-width and relative capacity improvement (see Figure 9). Some Ukrainian army units

*Figure 9*

## Relative capacity improvement of directional antennae

| Sender Beamwidth | Receiver Beamwidth | Relative Capacity Improvement |
|---|---|---|
| 20° | 20° | 324 |
| 30° | 30° | 144 |
| 90° | 90° | 16 |
| 20° | omni | 18 |
| 30° | omni | 12 |
| 90° | omni | 4 |

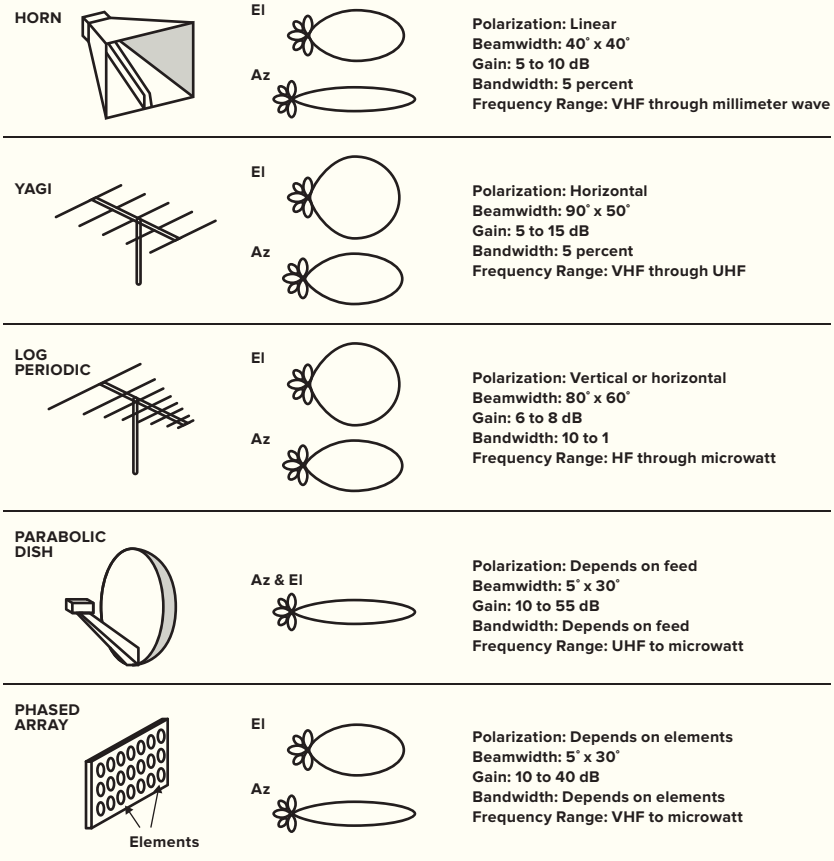
*Leland and Porche, Future Army Bandwidth Needs and Capabilities, p. 47.*

are using parabolic dish antennae to increase range between units.[126] Harris® currently sells a log periodic directional antenna (see Figure 10) that is compatible with VHF CNR.[127] Fielding of directional antennae would provide higher data rates for mission command systems, allow increased range and avoid the 360° exposure to jamming and direction finding.

The Army should consider phased array antennae, given their ability for rapid electronic steering to null out jamming signals and to narrow transmission beams between 5° and 30°, while also increasing transmission range (see Figure 10).[128] Additional solutions may include "smart" antennae that expand and

*Figure 10*

## Possible directional antennae for combat net radio with estimated horizontal (Az) and vertical (El) beamwidths

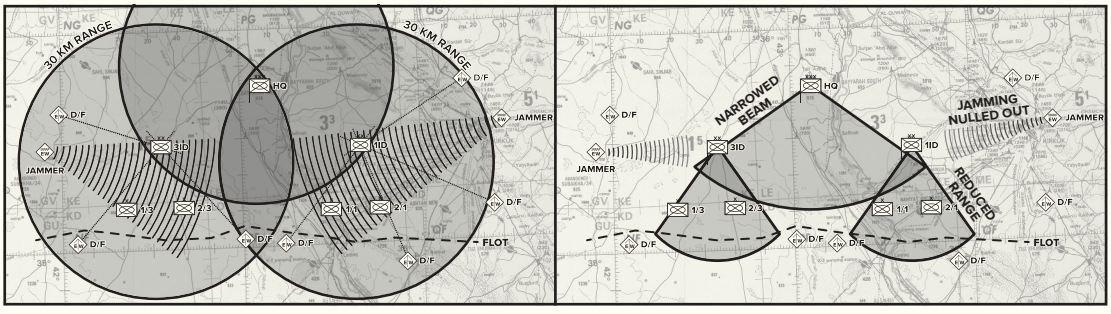



*Adapted from Adamy, EW 103, p. 58.*

contract their beams based on the locations of friendly units. Such antennae could also have a mode that automatically adjusts the power amplification based on the required range. Such characteristics would optimize CNR performance while minimizing exposure to electronic sensors (see Figure 11).

*Figure 11*

## Comparison of Omnidirectional Antennae with Directional Antennae




The omnidirectional antennae (left) at full range maximize exposure to direction finders (D/Fs) and jammers. Directional antennae (right) 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 "Operational Navigation Chart G-4, 1:1,000,000."*

Some platforms will require mostly omnidirectional transmission; 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 antennae connected to *friendly* direction finders. These direction finders would provide a line of bearing for each friendly transmission. With the receipt of each of these transmissions, the directional antenna or steerable null processor could adjust so that the antenna could send and receive 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 Fort Irwin, California, Fort Polk, Louisiana, 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; CTCs should be replicating the real fight as much as possible.

Units should routinely 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 antennae, radio silence and terrain masking while also forcing leaders and subordinates to understand the flexibility required to out-maneuver and outsmart EW attacks 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*[129]

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

The Army must not emulate the "lethargy of mind" to which the U.S. Navy succumbed in the Pacific against the Japanese Imperial Navy. The Army has already *anticipated* an enemy counterspace and EW threat; now it must readjust its equipment, training and doctrine to

prepare for that threat. The U.S. Army need not wait for a crisis to make this transition, but can instead develop a solution to the counterspace and EW threats before unprepared American troops face these challenges on an unforgiving field of battle.

## Endnotes

[1] Thucydides, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*, ed. Robert B. Strassler, trans. Richard Crawley (New York, NY: Free Press, 2008), pp. 40–41.

[2] Dan Lamothe, "'We Will Pay the Butcher's Bill in Blood': General Issues Stern Warning as He Becomes Army Chief," *Washington Post*, 14 August 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/.

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

[4] FM 3-55.93, *Long-Range Surveillance Unit Operations* (Washington, DC: Government Printing Office, 2009), p. 6-18.

[5] Michael R. Frater and M. J. Ryan, *Electronic Warfare for the Digitized Battlefield* (Boston, MA: Artech House, 2001), p. 48.

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

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

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

[9] *Ibid*., p. 202.

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

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

[12] Patrick J. Donahue and United States Army Forces Command, "Force Command Mission Command Network Priorities," 26 April 2016, pp. 1–3.

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

[14] Intelligence Science Board, "Integrated Sensor-Collected Intelligence" (Washington, DC: Department of Defense, 2008), p. 25.

[15] Kevin McCaney, "Army Still Catching Flak for Tactical Intell System," *Defense Systems*, 22 March 2016, https://defensesystems.com/articles/2016/03/22/army-dcgs-a- criticism.aspx.

[16] 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*, vol. 17, no. 1 and no. 53 (January 2010), p. 11.

[17] Gideon Rose, *How Wars End: Why We Always Fight the Last Battle* (New York, NY: Simon & Schuster, 2011), p. 18.

[18] Timothy Garden, *The Technology Trap: Science and the Military* (Exeter, United Kingdom: Brassey's Defence Publishers, 1989), p. 96.

[19] Byrne and Konyha, *Space Primer*, p. 188.

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

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

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

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

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

[25] Lockheed Martin, "Lockheed Martin MUOS Satellite Tests Show Extensive Reach in Polar Communications Capability," 31 January 2014, http://www.lockheedmartin.com/us/news/press-releases/2014/january/131-ss-muos.html.

[26] Director, Operational Test and Evaluation, "FY 2015 Annual Report," January 2016, p. 260.

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

[28] 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, p. 6, accessed 22 October 2016, http://www.gao.gov/assets/670/669930.pdf.

[29] Holly Zell, "Impacts of Strong Solar Flares," *NASA*, 7 June 2013, accessed 9 November 2016, http://www.nasa.gov/mission_pages/sunearth/news/flare-impacts.html.

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

[31] Tony Phillips, "Near Miss: The Solar Superstorm of July 2012," *NASA*, 23 July 2014, https://science.nasa.gov/science-news/science-at-nasa/2014/23jul_superstorm.

[32] Pete Riley, "On the Probability of Occurrence of Extreme Spaceweather Events," *Space Weather*, vol. 10 (2012), p. 1, accessed 13 November 2016, http://onlinelibrary.wiley.com/doi/10.1029/2011SW000734/epdf.

[33] Zell, "Impacts of Strong Solar Flares."

[34] Chapman, *Space Warfare and Defense*, pp. 203–4.

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

[36] Pillsbury, "China's Military Strategy toward the U.S.," p. 8.

[37] *Ibid*, p. 20.

[38] Huang Wen-Chi, "China's Space Capabilities and Their Regional Security Implications," (Carlisle, PA: U.S. Army War College, 2011), p. 55.

[39] Chapman, *Space Warfare and Defense*, p. 85.

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

[41] Chapman, *Space Warfare and Defense*, p. 85.

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

[43] USCC, "2015 Report to Congress of the United States–China Economic and Security Review Commission," 2015, p. 298, accessed 13 November 2016, http://www.uscc.gov/Annual_Reports/2015-annual-report-congress.

[44] Office of the Secretary of Defense, "Annual Report to Congress," 2016, p. 37.

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

[46] USCC, "2015 Report to Congress," p. 294.

[47] *Ibid*, p. 295.

[48] *Ibid*.

[49] Chapman, *Space Warfare and Defense*, p. 190.

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

[51] Bill Gertz, "Russia Conducts Fifth Test of New Anti-Satellite Missile," *Washington Free Beacon*, accessed 19 January 2017, http://freebeacon.com/national-security/Russia-conducts-fifth-test-new-anti-satellite-missile/.

[52] Ronald C. Wilgenbusch and Alan Heisig, "Command and Control Vulnerabilities to Communications Jamming," *Joint Forces Quarterly*, no. 69 (2013), p. 58.

[53] Wilgenbusch and Heisig, "Command and Control Vulnerabilities to Communications Jamming," p. 57.

[54] United States Government Accountability Office, "Defense Satellite Communications: DD Needs Additional Information to Improve Procurements" (Washington, DC: Government Printing Office, 2015), p. 2.

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

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

[57] Chapman, *Space Warfare and Defense*, p. 139.

[58] 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, p. 8.

[59] Shachtman, "Pentagon Paying China—Yes, China—To Carry Data."

[60] Deakin, *Battlespace Technologies*, p. 324.

[61] Chapman, *Space Warfare and Defense*, p. 139.

[62] 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, p. 6.

[63] Director, Operational Test and Evaluation, "Warfighter Information Network-Tactical (WIN-T) Increment 2, Second Follow-on Operational Test and Evaluation," 2015, p. iii.

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

[65] Director, Operational Test and Evaluation, "FY 2015 Annual Report," p. 136.

[66] James M. Rockwell, ed., *Tactical $C^3$ for the Ground Forces, AFCEA/SIGNAL Magazine $C^3I$ Series*, vol. 4 (Washington, DC: AFCEA International Press, 1986), p. 293. ECMs are "those actions taken to prevent effective use of the electromagnetic spectrum by an enemy (includes jamming and deception)."

[67] *Ibid*. ECCMs are "those actions taken to insure effective friendly use of the electromagnetic spectrum (despite hostile ECM efforts)."

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

[69] Lester W. Grau and Charles K. Bartles, "The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces (Draft)" (Fort Leavenworth, KS: Foreign Military Studies Office, 2016), p. 243.

[70] Adamy, *EW 103*, p. 197. Adamy's formula is 90 percent CEP=1.57*d* tan (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.

[71] FM 24-18, *Tactical Single-Channel Radio Communication Techniques* (Washington, DC: Government Printing Office, 1987), p. 6-2.

[72] Adamy, *EW 103*, pp. 190–91.

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

[74] Jeffrey S. Harley, "Reading the Enemy's Mail: Origins and Development of U.S. Army Tactical Radio Intelligence in World War II, European Theater of Operations" (Carlisle, PA: U.S. Army Command and General Staff College, 1993), p. 8.

[75] Jeffrey S. Harley, "Reading the Enemy's Mail," p. 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.

[76] Laurie G. Moe Buckhout, "Signal Security in the Ardennes Offensive: 1944–1945" (Carlisle, PA: U.S. Army Command and General Staff College, 1997), p. 31, accessed 12 October 2016, http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll2/id/829.

[77] Abdul Karim Baram, *Technology in Warfare: The Electronic Dimension* (Abu Dhabi, United Arab Emirates: The Emirates Center for Strategic Studies and Research, 2008), p. 409.

[78] 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 these short and rapid transmissions.

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

[80] Headquarters, Eighth Army, U.S. Army, "Field Order 17, Annex 5," 22 January 1945, p. 6, accessed 2 December 2016, http://cgsc.cdmhost.com/cdm/singleitem/collection/p4013coll8/id/3064/rec/2.

[81] Headquarters, 6th Infantry Division, U.S. Army, "Field Order 1, Annex XIII," 28 November 1944, p. 6, accessed 2 December 2016, http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll8/id/29.

[82] Headquarters, 5th Army, U.S. Army, "Outline Plan, Operation Shingle, Air Plan Communications," 12 January 1944, p. 5, accessed 2 December 2016, http://cgsc.cdmhost.com/cdm/singleitem/collection/p4013coll8/id/3942/rec/1.

[83] Robert D. Rood, "FM Tactical Communications under Intentional Interference" (Carlisle, PA: U.S. Army Command and General Staff College), p. 39, accessed 4 October 2016, http://cgsc.cdmhost.com/cdm/ref/collection/p4013coll2/id/1354.

[84] *Ibid*.

[85] FM 24-18, *Tactical Single-Channel Radio Communication Techniques*.

[86] *Ibid*., p. E-1.

[87] Adamy, *EW 103*, pp. 59–60.

[88] FM 24-18, *Tactical Single-Channel Radio Communication Techniques*, p. E-1. It is unknown if the SNAP-2 is still in inventory.

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

[90] Sterling, *Military Communications*, p. 412.

[91] FM 6-02.72, *Tactical Radios*, p. I-2.

[92] Adamy, *EW 103*, p. 157.

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

[94] Deakin, *Battlespace Technologies*, p. 386.

[95] Frater and Ryan, *Electronic Warfare for the Digitized Battlefield*, p. 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), p. 9.

[96] Baram, *Technology in Warfare*, p. 409.

[97] FM 11-1, *Talk II-SINCGARS* (Washington, DC: Government Printing Office, 1996), p. vii.

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

[99] FM 24-18, *Tactical Single-Channel Radio Communication Techniques*.

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

[101] FM 11-45, *Signal Support to Theater Operations* (Washington, DC: Government Printing Office, 1999).

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

[103] FM 3-38, *Cyber Electromagnetic Activities* (Washington, DC: Government Printing Office, 2014), p. 4-4.

[104] ATP 3-36, *Electronic Warfare Techniques* (Washington, DC: Government Printing Office, 2014), p. 1-2.

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

[106] Adamy, *EW 103*, p. 230.

[107] *Ibid*.

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

[109] Grau and Bartles, "The Russian Way of War," p. 241.

[110] Paul McCleary, "Russia's Winning the Electronic War," *Foreign Policy*, 21 October 2015, https://foreignpolicy.com/2015/10/21/Russia-winning-the-electronic-war.

[111] Grau and Bartles, "The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Ground Forces (Draft)," p. 245.

[112] Grau and Bartles, "The Russian Way of War," p. 244.

[113] Organization for Security and Co-operation in Europe, Special Monitoring Mission to Ukraine, "Camouflaged 'R-330ZH Zhitel' Jamming Station," 2016.

[114] Joint Multinational Training Group-Ukraine et al., "Lessons Learned from the UKR 1-24th Mech BDE" (Yavoriv, Ukraine: International Peacekeeping Security Center, 14 April 2016), p. 14.

[115] McCleary, "Russia's Winning the Electronic War."

[116] Phillip Karber and Joshua Thibeault, "Russia's New Generation Warfare," *The Potomac Foundation*, 13 May 2016, accessed 2 December 2016, http://www.thepotomacfoundation.org/Russias-new-generation-warfare-2.

[117] McCleary, "Russia's Winning the Electronic War."

[118] Sydney J. Freedberg, "Miserable, Disobedient & Victorious: Gen. Milley's Future U.S. Soldier," *Breaking Defense*, 5 October 2016, accessed 25 November 2016, http://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us- soldier.

[119] John Antal, "Simplify, Simplify, Simplify: An Update on the U.S. Army's Lower Tactical Internet Effort," *Military Technology*, February 2015, p. 84.

[120] Director, Operational Test and Evaluation, "FY 2015 Annual Report," p. 104.

[121] *Ibid*.

[122] Director, Operational Test and Evaluation, "Warfighter Information Network-Tactical (WIN-T) Increment 2, Second Follow-on Operational Test and Evaluation," pp. 29–30.

[123] Director, Operational Test and Evaluation, "FY 2015 Annual Report," p. 104.

[124] Henry S. Kenyon, "Gunnery Tool Hits the Mark," *SIGNAL Magazine*, March 2005, accessed 12 November 2016, http://www.afcea.org/content/?q=gunnery-tool-hits-mark.

[125] Leland and Porche, *Future Army Bandwidth Needs and Capabilities*, p. 48.

[126] Joint Multinational Training Group-Ukraine et al., "Lessons Learned from the UKR 1-24th Mech BDE," p. 15.

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

[128] Adamy, *EW 103*, pp. 63–65.

[129] Richard B. Frank, *Guadalcanal: The Definitive Account of the Landmark Battle* (New York, NY: Penguin Books, 1992), p. 605.