REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
21-04-2020	Master of Military Studies (MMS) thesis	AY 2019-2020

4. TITLE AND SUBTITLE
Beam Me Up: The U.S. Marine Corps and Communications by Light

5a. CONTRACT NUMBER
N/A

5b. GRANT NUMBER
N/A

5c. PROGRAM ELEMENT NUMBER
N/A

6. AUTHOR(S)
Mitchell, Nicholas S. (Major)

5d. PROJECT NUMBER
N/A

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER
N/A

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
USMC Command and Staff College
Marine Corps University
2076 South Street
Quantico, VA 22134-5068

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
N/A

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The United States Marine Corps needs to diversify its signature in the electromagnetic spectrum (EMS) by augmenting its radio frequency (RF) based equipment with light-based systems, using high-powered light-emitting diodes (LEDs), to be more survivable and realize increased communications assurance in an EMS contested environment against a peer or near-peer adversary.

15. SUBJECT TERMS
Electronic Warfare, EW, USMC, Marine Corps, electromagnetic spectrum, EMS, light-emitting diodes, LED, Russia, China

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			USMC Command and Staff College
Unclass	Unclass	Unclass	UU		19b. TELEPHONE NUMBER *(Include area code)* (703) 784-3330 (Admin Office)

United States Marine Corps
Command and Staff College
Marine Corps University
2076 South Street
Marine Corps Combat Development Command
Quantico, Virginia 22134-5068

MASTER OF MILITARY STUDIES

BEAM ME UP: THE U.S. MARINE CORPS AND COMMUNICATIONS BY LIGHT

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF MILITARY STUDIES

AUTHOR: MAJOR NICHOLAS MITCHELL

AY 2019-20

Mentor and Oral Defense Committee Member: Jorge Benitez, Ph.D.
Approved: _____//signed//_____
Date: _____21_April_2020_____

Oral Defense Committee Member: James Joyner, Ph.D. _____
Approved: _____//signed//_____
Date: _____21_April_2020_____

EXECUTIVE SUMMARY

Title: Beam Me Up: The Marine Corps and Communications by Light

Author: Major Nicholas Mitchell, United States Marine Corps

Thesis: The United States Marine Corps needs to diversify its signature in the electromagnetic spectrum (EMS) by augmenting its radio frequency (RF) based equipment with light-based systems, using high-powered light-emitting diodes (LEDs), to be more survivable and realize increased communications assurance in an EMS contested environment against a peer or near-peer adversary.

Discussion: Since World War II, militaries around the world have relied heavily on sensors and communication equipment based on the use of the RF portion of the EMS. Due to the characteristics of the RF spectrum, it is well suited for those applications, but it is also easily detectable by adversaries. In many cases it is detectable at distances which make Marines targetable at long ranges. While America has been engaged in the War on Terror, its great power competitors, namely Russia and China, have been investing in electronic warfare (EW) capabilities aimed at detecting, disrupting, and denying their adversaries use of the EMS. In potential future conflicts with America's great power competitors, Marines will be expected to survive within an enemy's weapons engagement zone (WEZ), while producing an RF signature detectable and targetable at long range runs counter to that expectation. Conventional thought about this problem revolves around the use of the EMS in a less detectable manner, using it at lower power, more directionally, or intermittently. Those ideas do address the need to be survivable within an enemy WEZ to some extent, but to the detriment of lethality. In order to not only survive, but thrive within an enemy WEZ, Marines must adopt changes that still allow them to shoot, move, and communicate. They must be able to gain and maintain the initiative and operate with greater tempo than the enemy. Augmenting RF communications with LED-based communications will allow Marines to communicate with a very low chance of detection. Additionally, LED-based communications can be used to replace data transmission cabling and allow for rapid emplacement and displacement of forces while avoiding the need to protect or conceal that cabling from enemy observation.

Conclusion: If the Marine Corps augments its current use of RF equipment with LED-based equipment, it will save lives by improving the survivability of Marine units within an enemy WEZ.

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE MARINE CORPS COMMAND AND STAFF COLLEGE OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT.

Figures

Page

Tables

Page

Table of Contents

Acknowledgments

As one of the seemingly few students at Command and Staff College who arrived without a master's degree, the Master of Military Studies (MMS) program was somewhat daunting. I had a general idea of what I wanted to write about, and the meet the mentors event helped me realize my lack of preparedness. The first question from most of the mentors was, "What is your thesis statement?" I had no idea, strike one. Most mentors were additionally not interested in the technical nature of my topic, strike two. Dr. Jorge Benitez, however, while also skeptical, agreed to give me a shot. I am grateful to Dr. Benitez for his mentorship, his professionalism, and his active participation in this project. I also thank Dr. James Joyner for his feedback and assistance in completing this MMS.

Introduction

Most Marine Corps communications depend on radio frequency (RF)-based equipment. The most common of these use beyond-line-of-sight (BLOS) long-distance High Frequency (HF), line-of-sight (LOS) Very High Frequency (VHF), and LOS Ultra High Frequency (UHF) which includes satellite communications (SATCOM). All of those means share several drawbacks. They all present electromagnetic signatures easily detectable by adversaries at long ranges. When unencrypted they can also be easily intercepted and exploited by adversaries. Whether encrypted or not, they are susceptible to jamming and effective nullification by adversaries. The most critical takeaway, however, is that in a peer or near-peer conflict, the Marine Corps' likely adversaries will be able to locate and subsequently target communication sources accurately. To be survivable within a Weapons Engagement Zone (WEZ), Marines must be less targetable. The United States Marine Corps needs to diversify its signature in the electromagnetic spectrum (EMS) by augmenting its RF based equipment with light-based systems, using high-powered light-emitting diodes (LEDs), to be more survivable and realize increased communications assurance in an EMS contested environment against a peer or near-peer adversary.

Figure 1 is a simple representation of the full EMS. Most military over-the-air communications occur between the HF and Extremely High Frequency (EHF) zones. All the frequencies between HF and EHF are part of the *radio* spectrum of the EMS and account for tactical voice communications, SATCOM, broadband microwave communications, tactical datalinks, and surveillance and fire-control radar systems. The equipment used for those functions is well known to America's adversaries. The specific operating frequencies of the equipment are also known, either from marketing materials or from covert surveillance. That should be no surprise as Bryan Clark and Mark Gunzinger point out in their 2017 Center for Strategic and Budgetary Assessments report, *Winning the Airwaves: Regaining America's*

Dominance In The Electromagnetic Spectrum, that militaries have been using RF-based communication and sensing systems which have not fundamentally changed since the beginning of World War II.[1] Clark and Gunzinger go on to argue that enduring advantages have proven "to be the product of new operational concepts and capabilities that enabled militaries to transition to the next phase of the electromagnetic (EM) warfare competition before their rivals."[2] Their ultimate argument is that the United States military needs to shift to that next phase of EM warfare by adopting a "low-to-no power approach," meaning low power countermeasures for passive and active sensors and Low Probability of Intercept / Detection (LPI / LPD) technologies for communications, and, where possible, no power (passive) for sensing.[3]

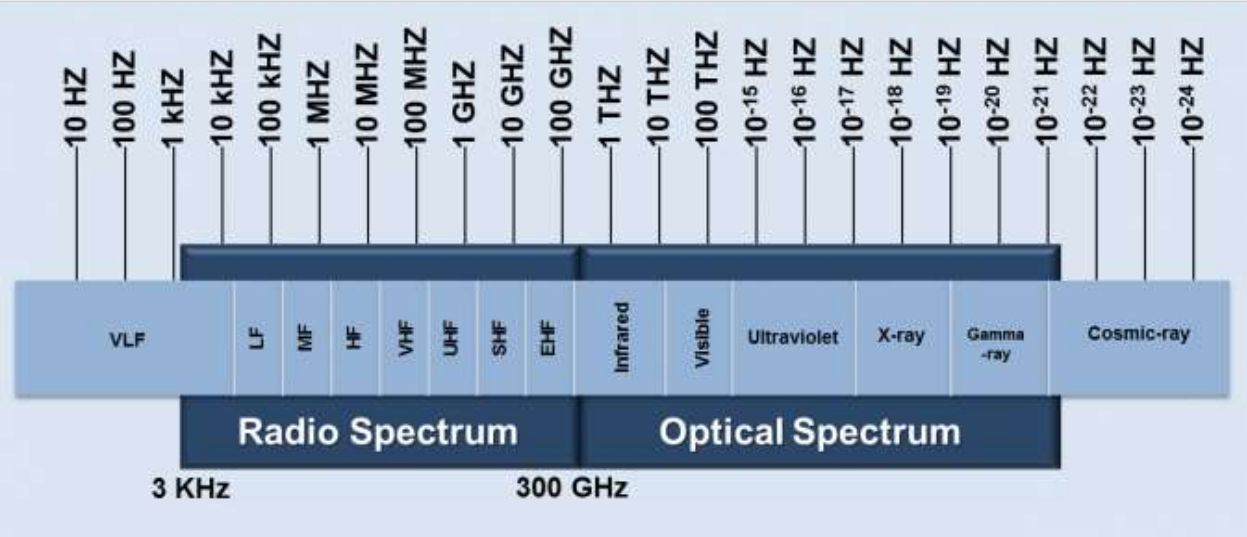

Figure 1: The full electromagnetic spectrum (EMS).[4]

The remainder of this paper will look to make the case that researchers like Clark and Gunzinger are correct about the American military's need to change their behavior with respect to the EMS. But they did not go far enough. China and Russia are proliferating equipment meant to locate, target and counteract everything in the radio spectrum. To move to a new phase of EM warfare competition it is not enough to simply use the old spectrum more quietly. The next phase will begin by jumping the divide between the *radio* and *optical* spectrums. Clark and Gunzinger

mention the ability to use LEDs for the sake of communications and sensing, but only as an afterthought to augment larger sensors.[5] Using LEDs for communication will give commanders flexibility in employing their equipment, it will create opportunities for rapid emplacement and displacement, and it will dramatically alter their EMS signature.

Vulnerabilities of USMC Communications

The US military is currently operating with a key vulnerability that can best be resolved with a dramatic shift in communications technology. The problem is stated rather succinctly by General David Berger in his *Commandant's Planning Guidance* by saying that in a peer or near-peer fight, namely against China or Russia, Marines must be able to "persist within range of adversary long-range fires . . . and sense, shoot, and sustain while combining the physical and information domains."[6] He goes on to say "Friendly forces must be able to disguise actions and intentions, as well as deceive the enemy, through the use of decoys, signature management, and signature reduction. **Preserving the ability to command and control in a contested information network environment is paramount**."[7] Many of the challenges presented in those few sentences tie directly back to the Marine Corps' reliance on RF communications, equipment generates very perceptible signatures that betray enormous amounts of information about its user and immediately make persisting within an adversary WEZ a dangerous proposition.

One of the primary problems with RF communications is the ease with which they can be detected by adversaries. Since military forces around the world have been relying on the spectrum since World War II, the characteristics of radio communications are well known by every developed nation in the world.

Another problem is that the radio spectrum is a rather finite resource. Figure 2, from the National Telecommunications and Information Administration (NTIA), shows how congested

the spectrum is. While that figure is not readable at this scale, it represents what would be only the HF portion of Figure 1. What is discernible, is that the HF spectrum has been divided up into very small chunks. None of the color-coding represents an unassigned segment and stacked colors represent multiple users. The full chart shows a similar division of the rest of the radio spectrum all the way up to 300GHz where the optical spectrum begins.

Figure 2: Specific breakdown of the HF spectrum.[8]

It would be easy for an adversary to use charts like those developed by the NTIA to quickly develop a rough understanding of what spectrum is available for use by the American military. Then they could combine that information with open source data from military radio equipment manufacturers and end up with a good idea of where to find American forces in the spectrum. With that information they could create purpose-built systems to target, disrupt, and exploit American systems at the time, place, and in the manner of their choosing.

The Great Power Threats

Russia, for example has made significant progress toward that end. In 2008, following their war with Georgia in which Russia lost an unsatisfactory number of airplanes to Georgian air defense systems, the Russian military initiated reforms aimed at more fully exploiting and developing significant use of the electromagnetic spectrum (EMS) by employing electronic warfare assets.[9] Between 2010 and 2013, Russia began to deliver on their promise to reform by testing and procuring improved systems.[10] Their longer range plans aim to result in electronic warfare (EW) forces becoming their own combat arm by 2025.[11] Table 1 details some of

Russia's emerging EW equipment. Many of the Russian systems are known to the West today due to their frequent use in Syria and Ukraine where they are continually battle tested.[12]

For example, Joe Gould sees evidence that "Ukrainian forces have grappled with formidable Russian electronic warfare capabilities that analysts say would prove withering even to the US ground forces."[13] He goes on to quote Lieutenant General Ben Hodges, then commander of U.S. Army Europe whose soldiers were training the Ukrainians at the time, as saying that the quality and capability of the Russians' EW was "eye watering."[14] According to Laurie Buckhout, the former chief of the U.S. Army's electronic warfare division, "Russia maintains an ability to destroy command-and-control networks by jamming radio communications, radars and GPS signals."[15] To put a fine point on the problem, Gould says that the Army isn't expected to field commensurate capabilities until 2023.[16]

Table 1: Russian EW systems and mission areas.[17]

System Name	Purpose
RB-301B Borisoglebsk-2	Automated jamming system (detection, direction finding, analysis and suppression of HF/VHF radio communications).
R-330Zh Zhitel	SATCOM/GPS/GSM jamming station (detection, direction-finding, analysis and suppression of UHF radio signals).
R-934UM	Radio jamming station (detection, direction-finding, analysis and suppression of VHF/UHF radio communications).
Pole-21	Designed to jam GPS signals.
RP-377LA Lorandit	Designed for detection, direction-finding and jamming of HF/VHF/UHF communications.
Leer-2	Designed to jam communications.
RB-341V Leer-3	Designed to jam GSM (2G cellular) networks. Includes a command post and three Orlan-10 UAVs equipped with jammers. Also capable of transmitting SMS messages to mobile phones.
RB-636M2 Svet-KU	Electronic protection/electromagnetic emission system. Designed for evaluation of electromagnetic situation. Conducts detection, analysis and direction-finding of emitting sources.

Similar capabilities are possessed by China and are in use in the Pacific.[18] According to a 2019 Center for Strategic and Budgetary Assessments study, China's People's Liberation Army (PLA), has initiated a modernization program which will include a comprehensive set of jammers and countermeasures targeted at American sensors and communications equipment.[19] For example, in 2015 China fielded the J-16D Red Eagle, their first purpose built EW aircraft which is comparable to the U.S. Navy's EA-18G Growler.[20] An aircraft like the J-16D gives China a platform capable of detecting, jamming, and targeting American communications and radar assets from long range. Additionally, given its fighter roots, the J-16D will be capable of escorting high-speed strike packages.[21] Additionally, China has installed "electronic warfare assets, which are designed to confuse or disable communications and radar systems" in addition to "anti-ship cruise missiles and surface-to-air missile systems, on three outposts in the hotly contested waters of the South China Sea".[22] Figure 3 is an example of China's military buildup in the South China Sea, it shows Woody Island which has been built up dramatically. The inset portion of Figure 3 is the same island in 2012 and shows that the northernmost green part of the island was barely connected to the main island and the space between that northern area and the runway was covered by water.[23] These represent just a few examples of China's preparation for a potential future conflict in the South China Sea, but they demonstrate China's desire to field a **comprehensive** set of countermeasures for America's current communications and sensors. Signature diversification is a must.

Figure 3: Woody Island is China's military headquarters in the South China Sea and is protected by fighter jets, surface-to-air missiles, and anti-ship cruise missiles. Photo: CSIS Asia Maritime Transparency Initiative/DigitalGlobe[24]

The above is only a sampling of threats and equipment, but it is plain to see that communications detection, direction-finding, and jamming are not afterthoughts to America's adversaries. According to John Hoehn, "The Russian military demonstrated its ability to pair EW drones with artillery fire, with devastating effects. According to U.S. intelligence sources, Russian forces used a single drone to provide intelligence for an artillery fire mission in July 2014 that resulted in the destruction of two Ukrainian battalions within minutes."[25] This supports the Marine Corps' *Electromagnetic Spectrum Operations (EMSO) Concept's* warning that future conflicts will be a "Battle of Signatures" and "Tomorrow's fights will involve conditions in which to be detected is to be targeted is to be killed."[26]

Self-Induced Vulnerabilities

Being detected and located by EW systems is a primary and relatively immediate threat to friendly units. However, in the event an adversary locates an emitter but chooses not to target

it, for instance if they have found an unencrypted communications channel, they can build a robust picture of what units and capabilities they are up against. This is an especially real consideration when considering HF/VHF/UHF communications. Virtually all HF/VHF/UHF radio nets in the Marine Corps provide for protection via encryption or frequency hopping. The protection, however, is dependent on the proficiency of each end user to either load the correct encryption key or hopping pattern into their radios.[27] When a user fails to do that correctly, they may elect to transmit in plain text while using previously agreed upon codewords to protect sensitive data. They should also use the brevity codes published by the multi-service Air Land Sea Application Center, although it may create a false sense of security since the brevity codes are meant explicitly for brevity and not for security.[28] Tactical radio nets, especially ones conveying time-sensitive information, like air control information, are frequently operated in this *user-encoded* instead of machine-encrypted manner.

Another reason a user may forego encrypted communications is that they also require more time to use since the encryption devices require a delay after beginning a transmission before the user may speak. Again, in the case of heavily congested air control nets, the delays associated with each transmission could significantly reduce the effectiveness of the net.

David Fiedler details how the North Vietnamese Army was able to exploit user-encoded radio nets to learn: artillery target information, artillery harassment and interdiction fire schedules, ambush site locations, casualty reports, air strike warnings, friendly troop positions, radio-net call sign and frequency changes, unit status reports, plans and orders, and idle operator chitchat containing all sorts of operational information.[29] Fiedler makes it clear that even against a seemingly non-technological adversary, a significant amount of information can be gleaned from unencrypted communications which can be costly on the battlefield. Communications with

user-selectable security options will always result in some level of reduced security and as a byproduct, risk to mission and risk to force.

The Threat of Jamming

An additional concern related to RF systems is their susceptibility to jamming. If an adversary is aware of friendly transmissions and is not targeting them reactively, they may instead be collecting a comprehensive friendly order of battle, identifying key nodes, communication nets, and sensors. With that information, they could launch a large-scale attack in which the use of vital sensors and communications were suddenly denied, and friendly forces were suddenly very vulnerable. This is the kind of comprehensive, coordinated attack that America unveiled in Operation Desert Storm. America's peer adversaries took notice. As Benjamin Lambeth put it:

> By the U.S. government's estimate, the heart of the Iraqi IADS was taken out within the first hour, and the entire system was "virtually destroyed" in 36 hours. Hardened SAM and interceptor operations centers were destroyed within four days. After that, individual air defense sectors were forced into autonomous operations. Throughout the air campaign, the E-3 AWACS, E-8 Joint Surveillance Targeting and Attack Radar System (JSTARS), and effective communications and radar jamming yielded a winning combination by expanding the coalition's situation awareness while denying it to the enemy. For this reason, Desert Storm has been rightly described by both Russian and Western experts as the first "information war"—and one in which electronic countermeasures moved decisively from a supporting role to a direct combat role.[30]

America's technological superiority over Iraq resulted in a severe overmatch. Today, America's closest competitors possess capabilities that might be able to similarly turn the tables. For example, Russian forces in Ukraine have demonstrated the capability to integrate unmanned intelligence, surveillance, and reconnaissance (ISR), electronic direction finding, standoff jamming and artillery fires.[31] Combining those capabilities allows the Russians to locate their targets with their inadvertent cooperation, disrupt their force protection counterbattery radar capabilities when they are needed most, and most importantly, deny the Ukrainians any

opportunity for effective retaliation. For years, the US military has been operating uncontested in the RF spectrum because it has been fighting non-state actors during the War on Terror. But just like the Ukrainians, the US military retains many dangerous vulnerabilities to the electronic warfare capabilities of a peer adversary such as Russia. America still needs to maintain its tried and true radio equipment and remain ready to punish its adversaries for their use of the RF spectrum, but America needs to take some of its eggs out of the RF basket. To be more specific, the Marine Corps, which expects its future fights to take place within its enemy's WEZ, needs to diversify its communications.

Improving the Survivability of US Marines Against Competitors with Advanced Electronic Warfare Capabilities

A readily available safeguard against an overreliance on the radio spectrum is to spread into the optical spectrum. More specifically, the Marine Corps should make use of light-based communications because light-based capabilities will help Marines reduce their EMS signature, be more maneuverable, and ultimately be able to persist within an enemy WEZ. Light-Emitting Diodes (LEDs), the same kind, albeit more powerful versions, found in the most energy efficient lighting in American homes are usable in the transmission of voice and data. LEDs can produce all the *frequencies* of the optical spectrum from infrared (IR) to ultraviolet (UV). The lowest IR frequencies start around 300Ghz, and the highest UV frequencies top out around 100,000THz. Which means there are thousands of times more spectrum available optically than in the entire congested radio spectrum.

This is not meant to diminish RF-based capabilities. Traditional radios have capabilities for very long-distance communication that LED communications simply cannot match. Due to its wavelength characteristics, HF communications can bounce between the ground and the

ionosphere and circle the globe. SATCOM can rapidly hop across space from the front lines of a conflict to other side of the world.

How can LEDs be used for communications though? Light-based communications work in virtually the same way as radios. Voltage is applied to a transmitting element, in this case an LED instead of an antenna, which excites photons and generates waves of radiation. The frequency of those waves determines the carrier signal, which effectively creates the path over which data can be transmitted. The most relatable comparison for this is the AM/FM radio in a car. AM Radio stations have carrier frequencies between 540 and 1600 kHz and FM stations range from 88 to 108 MHz. For radio communications, the receiving antenna can be identical to the transmitter. For light-based communications, a photoreceptor is used to receive the communications.

A photoreceptor is anything capable of detecting frequencies in the optical spectrum. The human eye is a photoreceptor in the visible spectrum and things like cameras have photoreceptors capable of seeing everything from IR to UV. Because the transmitter and receiver are distinct items, unlike a radio's dual-duty antenna, LED communications also provide the benefit of being full duplex, meaning users can transmit and receive simultaneously. This means users can communicate with one another in a more natural manner.

As mentioned previously, the colors of the optical spectrum are created by different frequencies. In much the same way an HF radio is defined by its ability to receive and transmit in the 2-30MHz frequency range, all the colors of the rainbow are determined by their frequency as well. Like radios, LED communications use an LED tuned to a specific frequency (color), which transmits information to a receiver (photoreceptor). One of the greatest benefits of LEDs though,

is that they can go beyond creating visible colors and can operate in *colors* that require special equipment to detect, which again refers to the IR and UV spectrum.

It's important to reiterate that a radio's antenna pulls double duty as the transmitting and receiving element while LED systems use LEDs to transmit and photoreceptors to receive. It is also important to note that adding a separate antenna to attempt simultaneous radio transmission and reception would result in self-jamming as transmitted signals would enter directly into the second antenna. When using the radio spectrum, even when using two antennas to separate the transmit and receive, it is also necessary to use two radios and distinct transmit and receive frequencies. With LED communications, so long as the sending unit's photoreceptor cannot see its associated transmitting LED, the system can transmit and receive simultaneously. This makes LED communication more like a typical phone call as opposed to the turn-based format of RF communications. That represents an immediate doubling of bandwidth. Figure 4 shows an example of a commercial side-by-side LED transmitter and receiver. Due to the parallel orientations of the transmitter and receiver, except for reflection, the system won't be susceptible to self-jamming.

Figure 4: The Torrey Pines Logic R50.[32]

Another important characteristic of the optical spectrum is that most of the wavelengths do not pass through solid objects. Whereas RF signals do pass through solid objects, consider Wi-Fi passing through the walls of a typical American home, emissions in the optical spectrum

can be blocked by a sheet of paper. Using light-based communications within a typical enclosed room would eliminate unintentional radiation outside of it. To achieve a similar blockage with the RF spectrum would require a grounded, fully metal enclosure, also known as a Faraday cage. Partially shielded systems using RF radiation intended to directionally focus their energy will still bleed energy in other directions. The bled energy has a lower probability of being detected than omnidirectional radiation, but it still creates an observable signature.

The emissions from LED communications on the other hand can be restricted by virtually any opaque substance and thereby precisely directed. This means that directional LED communications would have a very small probability of detection. Furthermore, if they were detected, they would be at a reduced risk compared to RF communications which are under threat of victim-guided anti-radiation munitions. When used directionally, LED communications present a narrow path between the sender and receiver which an attacking aircraft would have to enter for target acquisition. Combined with a lack of anti-radiation munitions designed to target optical spectrum frequencies, due to the limited use of the optical spectrum, LED systems provide significant enhancements to survivability.

Another benefit of LED communication is that it is inherently very jam resistant. The concept of jamming LED communications is substantially similar to that of RF systems. In either case, the jammer needs to overwhelm the receiving unit's receive element, whether that is an antenna or a photoreceptor, relative to the transmitter it wants to receive. To do that, a jammer must transmit a proportionally higher intensity signal than the friendly transmitter. In the case of a typical radio, a jammer located equidistant from the receiver must simply transmit an effectively higher power signal than the friendly transmitter to disrupt their communications. Varied distances will simply change the amount of power required from the jammer to create a

favorable ratio. Using directional antennas can create more favorable conditions for the jammer or the friendly parties. An important takeaway regarding RF jamming though, is that the relative orientations of the units is largely inconsequential since more power can always create a favorable jamming ratio.

It is much more difficult, however, to jam optical systems. The same way that a sheet of paper can prevent unintended light radiation from entering the environment, it can also prevent adversary radiation from reaching a friendly photoreceptor. In effect, light-communication can be so directional that for an adversary to interrupt it, they would have to either position themselves physically in between the sender and receiver, which would be easily detectable, or in line with, but behind either, the sender or receiver, and transmitting a proportionally more intense signal. In that case, the adversary system would be putting a very intense signal into the environment and because of the directionality previously mentioned, they may only be able to impact a single link. If frontline ground users were using such a system to communicate to airborne nodes located to their rear, the geometries required to jam those links would be all but impossible to achieve.

Figure 5 depicts the geometries associated with detecting and interfering with LED communications. The shaded area on the left represents enemy territory and units A and B represent the forward most friendly ground units. Unit C represents a rearward airborne communications relay. Assuming good local security, the only way for an adversary to intercept or disrupt communications between units A and B would be to take a position between them like unit D. To similarly impact communications between units A or B and unit C, would require that an adversary take up a position between them and at a lower altitude than unit C, as depicted by unit F, or at a higher altitude and behind unit C, as depicted by unit E. In both of those situations,

the enemy platform must operate behind friendly lines and maintain their position between the sender and receiver. Neither of those scenarios is realistic. Additionally, unit G, which could arguably be operating close enough to identify and locate RF systems, would have virtually no chance of detecting LED communications at these geometries.

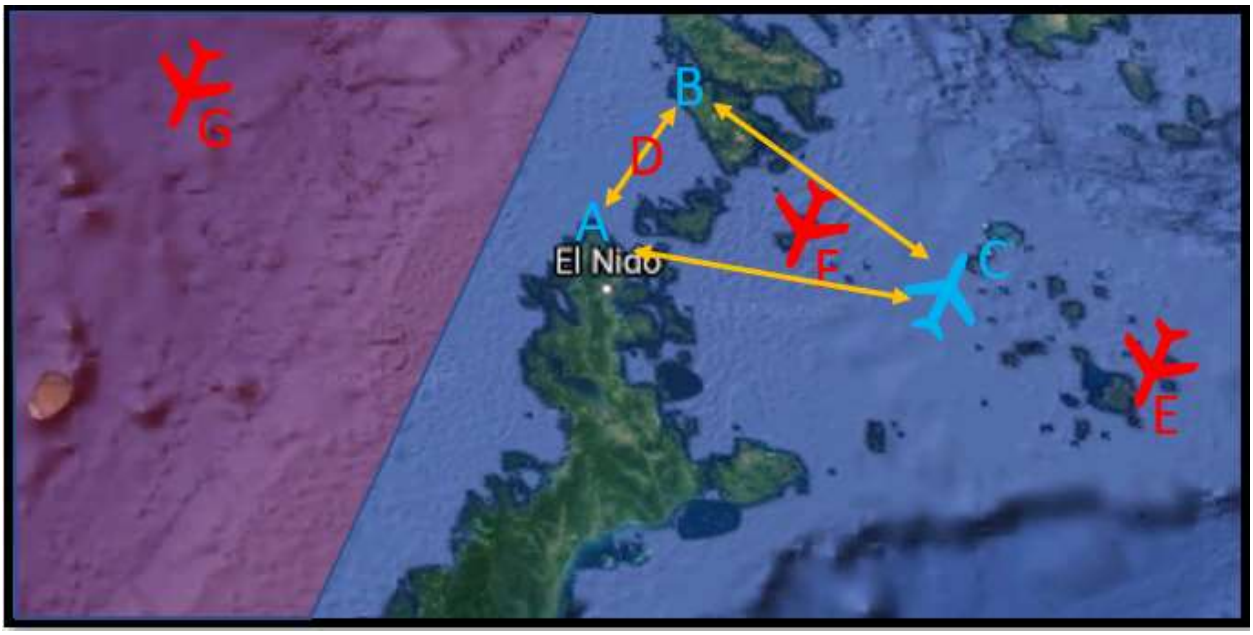

Figure 5: Diagram of interception or jamming geometries.

Due to its non-visible nature, many LED communications systems tout their use of the IR spectrum as an attractive feature. Detractors of IR LED communications could argue that IR jammers exist much like RF jammers and that LED communications can be interrupted as easily as RF communications can be. However, while there are in fact systems marketed as IR jammers, and installed on military platforms, they are invariably IR countermeasures. They are intended to confuse weapons with IR homing systems and would be ineffective against the type of communications described in this document. Figure 6 is the BAE systems AN/ALQ-144 which is an example of an IR countermeasure commonly installed on rotary-wing aircraft.

Figure 6: AN/ALQ-144 Infrared Countermeasure[33]

Size, Weight, and Power

Another benefit of LED based communication is the Size, Weight and Power (SWaP) of the components. It is necessary at this point to remember that although the components present moderate SWaP costs, all the costs are additive to current equipment sets. A SWaP comparison of the Torrey Pines Logic R50 in figure 4 and a L3Harris PRC-117G is as close to an apples-to-apples comparison as possible. The PRC-117G is presented in figure 7. The R50 is one of the largest offerings from Torrey Pines Logic, offering the longest range, and highest data throughput, and the PRC-117G is a very capable, widely proliferated tactical radio. It also happens to be among the smallest of tactical radios.

Figure 7: PRC-117G.[34]

The first area of comparison is its size. The R50 measures 9.5” x 8.5” x 8.5”, which equates to .4 cubic feet.[35] The PRC-117G with battery attached measures 3.7” x 7.4” x 8.8”, which equates to .14 cubic feet.[36] While that may look like a big win for the 117G, it doesn’t account for a minimum 12” antenna protruding from the face. The second area is weight. The R50 weighs in at 6 pounds.[37] The PRC-117G weighs in at 8.2 pounds or 12 with its battery.[38] That is pretty favorable considering just how small the 117G is. Finally, the comparison of power consumption. The R50 requires a 5-12-volt, direct current (DC), 10-watt power supply.[39] The 117G requires a 24.5-volt DC, 60-watt power supply.[40] Since watts are the real measure of energy usage, the R50 wins in that category by a factor of 6, but there are arguably more important areas for comparison.

Data Throughput

One such area is in data throughput. The 117G is very capable in the data realm. It was one of the first radios to use the Adaptive Networking Wideband Waveform Revision C (ANW2C). ANW2C allows the 117G to act like a wireless router and pass data between radios. That data can be used just like an internet connection to communicate. It is possible to have a simple two node network generating 2Mbps of throughput all the way up to a network of thirty

nodes sharing 10Mbps of throughput.[41] According to one account from Afghanistan in which a 117G was put aboard an aerostat, elevating it several hundred feet in the air, a usable ANW2C range of forty kilometers was achieved.[42] The R50 on the other hand can provide up to 20Mbps between two nodes and advertises a range capability of 10+ kilometers. Considering that a high-quality voice over internet protocol (VOIP) phone call uses ~64kbps of data, 20Mbps can support a lot of communication.[43]

A more important comparison, however, might be to compare the data throughput to Link-16. Link-16 is a theater-wide datalink, spanning up to a 300-mile area. Link-16 is used heavily by aviation units and provides situational awareness by displaying friendly unit locations along with friendly sensor data. In a major theater, Link-16 can support hundreds of users and generate a comprehensive air tactical picture, which in turn feeds the Common Operational Picture (COP). Figure 8 shows the wide variety of users on Link-16 and illustrates the point that Link-16 is a robust data link with a lot of information. However, a full Link-16 network still only generates 1Mbps of data. Another important note is that the 300-mile range mentioned previously is a physical limitation based on the extent of radio signal propagation possible without breaking the network timing. That opens the door for things like Joint Range Extension Application Protocol – C (JREAP-C), which is a TCP/IP extension of Link-16. The high data throughput available with LED communications could allow for extended use of this vital command and control data link as the RF version is threatened by America's adversaries.

Figure 8: Graphic depiction of Link-16 network.[44]

Cost

A main area of concern when discussing emerging technologies of course is the price tag. To buy a single very basic R50, capable of transmitting data 5-6 times the visible limit, or up to 10 kilometers in clear conditions at data rates of up to 20Mbps would cost about $10,000.[45] That would essentially be an exquisite piece of equipment and account for zero economies of scale. According to the Department of Defense Fiscal Year 2018 Budget Estimates for Procurement, Marine Corps, in 2017, the Marine Corps purchased 73 PRC-117Gs for a total of $2.546 million. That equates to $34,879.71 per radio.[46] The 2019 Budget had some disagreement with the 2017 data indicating that the Marine Corps purchased 429 radios with some capability variation, but they still averaged $34,969.69.[47] That makes the R50 worth at least 3.5 PRC-117Gs and doesn't account for the costs associated with adding things like antennas, enhanced waveforms, handsets, vehicle adapters, and power amplifiers that can easily run into the tens of thousands of dollars.[48]

Transmission Limitations

So far LED communications may seem like a bit of a panacea for communications assurance and signature management applications. Which is why it is important to remember when comparing the capabilities of something like the R50 and a 117G, that the effective range

is important. As previously discussed, the 117G can establish a data network over the air that can reach upwards of forty kilometers compared to the R50's ten kilometers. Those numbers can be misleading since the 117G's performance will be minimally impacted by environmental factors while the R50 works best in favorable conditions. According to the R50 datasheet, when the system is operating in reduced visibility, its range is reduced to 5-6 times the visible limit.[49] Dense fog would qualify as reduced visibility and according to the AccuWeather website, dense fog is defined as reducing visibility below a quarter mile.[50] That would reduce the R50's range to a mile and a half or less. On the positive side though, fog impacts friendly forces the same as foes. It might also seem like this would allow for an adversary to suppress friendly communications with obscurants like smoke, but IR frequencies are much less affected by smoke than by fog.[51]

On that note, it is also important to note that not all optical frequencies are created equally. Figure 9 for example depicts the capability of IR frequencies to penetrate the atmosphere. The x-axis represents the frequency wavelength in microns and the y-axis represents the percent of penetration. The higher peaks on the graph indicate greater atmospheric penetration and show that there are portions of the IR spectrum that would be effective for data transmission, even in adverse conditions.

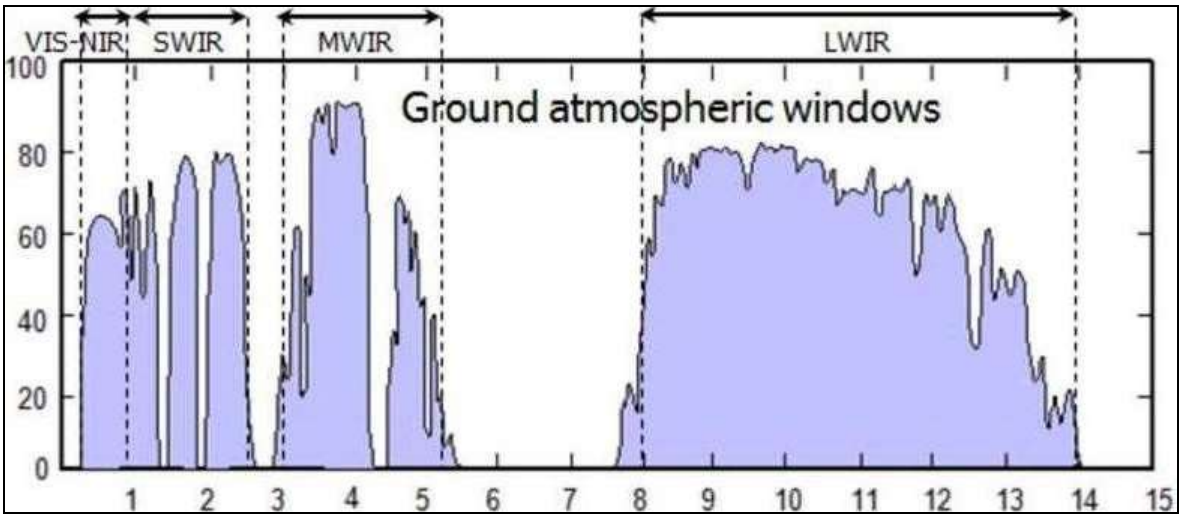

Figure 9: IR Atmospheric Transmittance.[52]

Naval Integration and Implementation

Most of the comparison has been between a 117G using ANW2C and an R50 conducting data transfers. This is not to disregard or belittle the capability of the 117G to conduct single channel voice communications or SATCOM, but a robust data path is worth numerous RF links. In the Navy's *A Design for Maintaining Maritime Superiority 2.0*, they lay out a plan to design and implement a comprehensive network to support Distributed Maritime Operations including tactical grid connections to distributed units.[53] What this tactical grid will eventually look like is anyone's guess, but a fair guess is that it will include distributed unmanned airborne network access points. If the distributed units were to connect to these airborne access points using LED communications, they could effectively shift all their traditional electromagnetic signature risks to a much more survivable and risk-worthy platform without compromising their situational awareness.

The idea of the Navy using LED communications as part of its network architecture is not far-fetched. In fact, the Navy may be the only service with a current program of record using LED communications. The Navy currently uses the AN/PAQ-6 Phone & Distance Line Replacement, also made by Torrey Pines Logic, in its underway replenishment operations.[54] The

PAQ-6 allows ships in close proximity to share phone lines, data connections, and enjoy a constant update on the distance between them. These connections allow for wireless voice, video, and data connections even while operating under Emissions Control (EMCON) conditions.

Enhancements to Concealment and Manueverability

So far, this document has made the case for LED communications based on their ability to transmit and receive data between units. But LEDs offer benefits within units as well. They contribute particularly to the force protection and maneuverability of units like command and control (C2) agencies. A specific example for today would be a Tactical Air Operations Center (TAOC). TAOCs currently use a wide array of systems and equipment that generate battlespace awareness and actively manage the air portion of the battlespace. Unfortunately, they also generate a huge electromagnetic signature and their exquisite equipment represents very lucrative targets. LED communications could be used to improve the survivability of TAOC systems. Their equipment sets are typically geographically dispersed, spreading out their surveillance radar, communications vehicles, and operations facility as much as possible. A major drawback to dispersing the equipment is that they still share data over physical cabling. Those cables have to be run between each node and in the case of the AN/TPS-80 Ground / Air Task-Oriented Radar (G/ATOR), running that cable a tactically relevant distance, a kilometer or more, is the most time consuming task during emplacement or displacement. This is where LEDs provide time and value. Instead of running cables, the various dispersed pieces of equipment would run their data cable to something like the R50 which would beam its data to the central node. The R50 is perfectly suited to airgap this sort of network connection. This would allow the G/ATOR to take advantage of its rapid setup and teardown capability and present no more than a fleeting opportunity for an enemy to engage it. A variant of the G/ATOR is also being fielded to

the Marine artillery community as their new counterbattery sensor and every bit of tempo they can achieve will reduce their extreme vulnerability against a peer adversary fighting in the EMS.

In addition to enhancing the speed at which equipment can be set up and networked together, LED connected equipment would also be able to set up in configurations that were previously impossible. For example, a radar could be deployed more than two kilometers from its C2 agency, or it could be deployed across a body of water which a cable could not have been laid across in the past. The survivability that comes with being able to hide a C2 agency and then remote their equipment with the most detectable electromagnetic signatures would be dramatic. It would still be dangerous for Marines on the distant end, operating that equipment, but tactics, techniques, and procedures including intermittent radiation and regular displacement could mitigate that risk. Another benefit to wirelessly transmitting data is that it eliminates the need for expensive cables.

Fiber optic cabling in the kilometer and longer ranges costs between $2,700 for single-mode cable and $3,800 for multi-mode per kilometer.[55] The difference between single-mode and multi-mode is beyond the scope of this paper, but suffice it to say that the Marine Corps uses both types for various systems and the cable cost alone would offset much of the replacement cost of R50s.[56] To return to the TAOC example, they keep at least two kilometers of cable per remote system on hand at all times. Because of the on-hand cable limitations, two kilometers is about the furthest possible dispersion between major equipment sets. Even in dense fog with a mile and a quarter to a mile and a half of range, LEDs could match the legacy range of two kilometers and still be capable of an impressive ten kilometers in good weather.

Additionally, the size and weight portions of SWaP for an R50 compared to a cable is more pronounced. For example, a typical 500-meter fiber optic reel takes up approximately 1.4

cubic feet of space.[57] That makes it 3.5 times bulkier than the .4 cubic foot R50. The reel itself also weighs 11.5 pounds, which is nearly double that of an R50.[58] Adding 500 meters of cable at approximately 17 pounds makes a typical 500-meter cable assembly weigh 28.5 pounds.[59] To continue down this line, it would take four of these cable assemblies to equal two kilometers of cable which would weigh 114 pounds and take up 5.6 cubic feet of space, compared to the two R50s that could do the same job for 12 pounds and .8 cubic feet. To take this to its logical conclusion in terms of a single MACCS agency, the TAOC, which deploys with at least one radar, one Composite Tracking Network (CTN), and two MRQ-13s (communications trucks containing standard radios); there is an opportunity to exchange 456 pounds of cabling, taking up 22.4 cubic feet of space, for 8 R50s at a total of 48 pounds and 3.2 cubic feet. That's a savings of 400 pounds and nearly 20 cubic feet, which is about the same as the space taken up by the largest washing machine available at The Home Depot compared to an average microwave oven.

TAOC Marines spend hours laying each fiber between their various pieces of equipment. They must take care to lay it out of the way of foot and vehicle traffic to avoid damage, and they often mark it with engineer tape and glowsticks. Across open desert it is sometimes laid directly on the ground, creating unnatural lines, visible to reconnaissance, and vulnerable to destruction by wildlife. Conversely, burying fiber across open desert, creates similarly unnatural lines in the environment. In either situation, radials pointing back to the heart of the C2 agency would be created. Those lines take hours to set up and hours to tear down. In the future threat environment, friendly forces need to be able to emplace, operate, and displace within the enemy's targeting cycle and physical cables simply don't support that. Thus, adding LED communications capabilities would provide speed and invaluable time for Command and Control units.

There is still another benefit to using light-based communications that has not been discussed thus far. Unlike the RF spectrum, the optical spectrum is not regulated.[60] The type of spectrum division from figure 2 does not exist in the optical spectrum. This means that the use of the optical spectrum, apart from being smart from a signature management perspective, might also allow for greater training opportunities in spectrum congested areas. This could be particularly useful for units stationed overseas where the difficulty in securing spectrum access is multiplied by foreign regulatory bodies.

Conclusion

In 2019 , the Commandant of the Marine Corps, General David Berger, listed signature management, mobile air defense, and expeditionary airfield capabilities and structure to support manned and unmanned aircraft and other systems from austere, minimally developed locations as areas in which the Marine Corps is under-invested.[61] Mobile air defense and expeditionary airfield operations are literally in the same community as the TAOC and signature management is the main point of highlighting this capability. Light communications may offer a good starting point in reducing some of the largest signatures in the Marine Corps and support the previous Commandant, General Neller's thought that, "the number one priority is resilient, survivable, reliable command and control."[62] As it said in the Joint Operating Environment 2035, the future environment will be a "contest of "hiders" vs. "finders" on the battlefield.[63] Every bit of advantage that the Marine Corps can gain over its enemies in this deadly game of hide and seek might be decisive and determine which side is victorious in battle.

As mentioned previously, LED communications are not the proverbial silver bullet that will solve the Marine Corps' signature management problems. They will not allow Marines to operate undetected and with impunity in hostile territory. The argument presented here is that in contested EW environments, the use of LED communications will reduce the odds of Marines

producing a signal detectable and therefore targetable at long range. In addition, LED communications may allow for significantly faster emplacement and displacement of the Marine Corps' cable-dependent exquisite systems. Nevertheless, on their own, LED communications will not even solve all the signature management issues of the TAOC. The prevalence of satellite-based capabilities, especially in the cases of Russia and China, would require extensive camouflage and the management of signatures all the way down to the heat given off by generators.

As explained, there are many reasons why the Marine Corps should augment its traditional communications equipment with LED-based communications equipment. Due to advancing threat capabilities, the Marine Corps is concerned with its ability to manage its signature in the EMS, from the Commandant on down. The dominant thinking in regard to achieving that revolves around minimizing the Marine Corps' EMS signature by transmitting at lower power, with greater directionality, and in shorter, more intermittent bursts. Doing those things will achieve greater survivability in an enemy WEZ, but at the cost of lethality. In the current threat environment, LED-based communications would allow Marines to continue to communicate freely. Marines would be able to share information, maintain situational awareness, and in many cases even emplace and displace more rapidly. That means instead of silently hiding to survive in an enemy WEZ, Marines would regain their ability to shoot, move, and communicate and be lethal and survivable.

Bibliography

Air Land Sea Application Center. Brevity Multiservice Tactics Techniques and Procedures. MCRP 3-30B.1. Langley, VA: Air Land Sea Application Center, June 2018.

Berger, David. Notes on Designing the Marine Corps of The Future. https://warontherocks.com/2019/12/notes-on-designing-the-marine-corps-of-the-future/.

Berger, David. Commandant's Planning Guidance Washington D.C: U.S. Marine Corps, July 17, 2019.

Clark, Bryan and Mark Gunzinger. Winning the Airwaves: Regaining America's Dominance in the Electromagnetic Spectrum. Center for Strategic Budgetary Assessments. 2017.

Clark, Bryan, Whitney M. McNamara, Timothy A. Walton. Winning the Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum. Center for Strategic Budgetary Assessments.

Department of Defense Fiscal Year (FY) 2018 Budget Estimates. Procurement, Marine Corps. May 2017. https://www.secnav.navy.mil/fmc/fmb/Documents/18pres/PMC_Book.pdf.

Department of Defense Fiscal Year (FY) 2019 Budget Estimates. Procurement, Marine Corps. February 2018. https://www.secnav.navy.mil/fmc/fmb/Documents/19pres/PMC_Book.pdf.

Fiedler, David. "Project Touchdown: How We Paid the Price for Lack of Comsec in Vietnam." Infantry 93, no. 5 (September 2004): 19-22.

Freedberg Jr., Sydney J. Marines Need Submarines: Commandant Neller On Major War. https://breakingdefense.com/2018/02/marines-need-submarines-commandant-neller-on-major-war/

Gould, Joe. Electronic Warfare: What US Army Can Learn From Ukraine. August 2, 2015. https://www.defensenews.com/home/2015/08/02/electronic-warfare-what-us-army-can-learn-from-ukraine/.

Gu, Kevin. How Much Data Does VOIP Use? January 28, 2019. https://www.genvoice.net/how-much-data-does-voip-use/

Hoehn, John. Ground Electronic Warfare: Background and Issues for Congress. Congressional Research Service. September 17, 2019.

Lambeth, Benjamin S. The Winning of Air Supremacy in Operation Desert Storm. RAND. 1993.

Amanda Macias. China is Quietly Conducting Electronic Warfare Tests in the South China Sea. July 5, 2018. https://www.cnbc.com/2018/07/05/us-intel-report-china-quietly-testing-electronic-warfare-assets-on-sp.html.

Marine Corps Concept for Electromagnetic Spectrum Operations. Washington D.C: U.S. Marine Corps. October 18, 2017.

McDermott, Roger N. Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. 2017.

McDermott, Roger N. Russia's Advances in Electronic Warfare Capability. October 4, 2019. https://www.realcleardefense.com/articles/2019/10/04/russias_advances_in_electronic_warfare_capability_114786.html

Pomerleau, Mark. Breaking Down China's Electronic Warfare Tactics. March 22, 2017. https://www.c4isrnet.com/c2-comms/2017/03/22/breaking-down-chinas-electronic-warfare-tactics/

Roblin, Sebastien. Why China's J-16D Electronic Warfare Plane Is a Really Big Deal. November 20, 2019. https://nationalinterest.org/blog/buzz/why-chinas-j-16d-electronic-warfare-plane-really-big-deal-97677.

Richardson, John. A Design for Maintaining Maritime Superiority 2.0. Department of the Navy. December 2018.

Sanchez, Simon. "Mesh Networking in the Tactical Environment Using White Space Technology". Monterey, California: Naval Postgraduate School. December 2015.

Scott, Kevin D, and Joint Chiefs of Staff Washington United States. Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World, July 14, 2016. http://www.dtic.mil/docs/citations/AD1014117.

Seffers, George. "THE LITTLE RADIO THAT COULD." Signal 66, no. 3 (November 1, 2011): 31–33. http://search.proquest.com/docview/908614842/.

Trevithick, Joseph. Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio "Virus". October 30, 2019. https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus.

Tuthill, Samantha-Rae. What is the Dense Fog Advisory? June 22, 2012. https://www.accuweather.com/en/weather-news/what-is-the-dense-fog-advisory/223402

[1] Bryan Clark and Mark Gunzinger. Winning the Airwaves: Regaining America's Dominance in the Electromagnetic Spectrum. Center for Strategic Budgetary Assessments. 2017. i.
[2] Bryan Clark and Mark Gunzinger. ii.
[3] Bryan Clark and Mark Gunzinger. ii.
[4] https://www.nasa.gov/content/electromagnetic-spectrum/
[5] Bryan Clark and Mark Gunzinger. 34.
[6] Commandant's Planning Guidance. July 17, 2019. 12.
[7] Commandant's Planning Guidance. July 17, 2019. 12.
[8] https://www.ntia.doc.gov/files/ntia/publications/2003-allochrt.pdf
[9] Roger N. McDermott, Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum. 2017. 1.
[10] Roger N. McDermott, Russia's Electronic Warfare Capabilities to 2025. 13.
[11] Roger N. McDermott, Russia's Electronic Warfare Capabilities to 2025. 10.
[12] Roger N. McDermott. Russia's Advances in Electronic Warfare Capability. October 4, 2019. https://www.realcleardefense.com/articles/2019/10/04/russias_advances_in_electronic_warfare_capability_114786.html
[13] Joe Gould. Electronic Warfare: What US Army Can Learn From china. August 2, 2015. https://www.defensenews.com/home/2015/08/02/electronic-warfare-what-us-army-can-learn-from-ukraine/.
[14] Joe Gould. Electronic Warfare: What US Army Can Learn From Ukraine.
[15] Joe Gould. Electronic Warfare: What US Army Can Learn From Ukraine.
[16] Joe Gould. Electronic Warfare: What US Army Can Learn From Ukraine.
[17] Roger N. McDermott, Russia's Electronic Warfare Capabilities to 2025. B-1.
[18] Mark Pomerleau. Breaking down China's electronic warfare tactics. March 22, 2017. https://www.c4isrnet.com/c2-comms/2017/03/22/breaking-down-chinas-electronic-warfare-tactics/
[19] Bryan Clark, Whitney Morgan McNamara, Timothy a. Walton. Winning the Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum. Center for Strategic Budgetary Assessments. 19.
[20] Sebastien Roblin. Why China's J-16D Electronic Warfare Plane Is a Really Big Deal. November 20, 2019. https://nationalinterest.org/blog/buzz/why-chinas-j-16d-electronic-warfare-plane-really-big-deal-97677.
[21] Sebastien Roblin.
[22] Amanda Macias. China is Quietly Conducting Electronic Warfare Tests in the South China Sea. July 5, 2018. https://www.cnbc.com/2018/07/05/us-intel-report-china-quietly-testing-electronic-warfare-assets-on-sp.html.
[23] Amanda Macias. China is Quietly Conducting Electronic Warfare Tests in the South China Sea.
[24] Amanda Macias. China is Quietly Conducting Electronic Warfare Tests in the South China Sea.
[25] John Hoehn. Ground Electronic Warfare: Background and Issues for Congress. Congressional Research Service. September 17, 2019. 4.
[26] Marine Corps Concept for Electromagnetic Spectrum Operations. Department of Defense. October 18, 2017. 3.
[27] The hopping pattern for a radio refers to radios which can operate in modes like HaveQuick or SINCGARS (Single Channel Ground and Airborne Radio System) in which the radio rapidly changes its frequency to avoid being jammable on a single frequency. The frequencies used and the order of progression are known to all participants and the system time of participating radios must be synchronized. This information can be loaded into a radio in much the same way that an encryption key is transmitted into a radio's encryption device. Radio operators who are not proficient in loading encryption are probably also not proficient in loading hopping patterns and will tend to resort to plain text operations.
[28] ALSA Brevity. 3. The terms in the brevity manual are intended to help convey information as rapidly as possible. For instance, the word TALLY means "Sighting of a target, nonfriendly aircraft, or enemy position" which if stated over a plain text frequency might alert an enemy to the fact that it has been compromised. The term PLAYTIME means "Amount of time aircraft can remain on station, given in hours plus minutes" which conveys potential friendly vulnerabilities. The brevity terms taken together can betray an enormous amount of friendly information related to composition, disposition, and strength. Since the brevity manual is a readily accessible unclassified document it should be assumed that enemy forces are familiar with it.
[29] David Fiedler. "Project Touchdown: How We Paid the Price for Lack of Comsec in Vietnam." Infantry 93, no. 5 (September 2004): 19–22.
[30] Benjamin S. Lambeth. The Winning of Air Supremacy in Operation Desert Storm. RAND. 1993. 5.

[31] Joseph Trevithick. Ukrainian Officer Details Russian Electronic Warfare Tactics Including Radio "Virus". October 30, 2019. https://www.thedrive.com/the-war-zone/30741/ukrainian-officer-details-russian-electronic-warfare-tactics-including-radio-virus.
[32] https://tplogic.com/lightspeed-r50/
[33] https://www.baesystems.com/en-us/product/analq144-infrared-countermeasures-set
[34] https://www.harris.com/solution/harris-falcon-iii-an-prc-117gv1c-multiband-networking-manpack-radio
[35] Torrey Pines Logic R50 datasheet. https://tplogic.com/wp-content/uploads/2019/08/lightspeed_r50.pdf.
[36] L3HARRIS FALCON III® AN/PRC-117G(V)1(C) datasheet. https://www.harris.com/sites/default/files/downloads/solutions/an-prc-117g-multiband-networking-manpack-radio-datasheet.pdf
[37] Torrey Pines Logic R50 datasheet.
[38] L3HARRIS FALCON III® AN/PRC-117G(V)1(C) datasheet.
[39] Torrey Pines Logic R50 datasheet.
[40] L3HARRIS FALCON III® AN/PRC-117G(V)1(C) datasheet.
[41] Simon Sanchez. "Mesh Networking in the Tactical Environment Using White Space Technology". Monterey, California: Naval Postgraduate School. December 2015. 9.
[42] George I. Seffers. The Little Radio That Could. November 2011. 32.
[43] Kevin Gu. How Much Data Does VOIP Use? January 28, 2019. https://www.genvoice.net/how-much-data-does-voip-use/
[44] https://missiledefenseadvocacy.org/defense-systems/link-16/
[45] Email from Leo Volfson, President of Torrey Pines Logic dated January 21, 2019.
[46] https://www.secnav.navy.mil/fmc/fmb/Documents/18pres/PMC_Book.pdf. 245.
[47] https://www.secnav.navy.mil/fmc/fmb/Documents/19pres/PMC_Book.pdf. 340.
[48] https://www.gsaadvantage.gov/ref_text/GS35F0163N/0SK85N.3LCH66_GS-35F-0163N_GS35F0163N.PDF. 31. GSA Advantage is one of a select few vendors available for the DoD to order equipment. The items prefaced with RF-7800M are examples of accessories for the PRC-117G.
[49] Torrey Pines Logic R50 datasheet.
[50] Samantha-Rae Tuthill. What is the Dense Fog Advisory? June 22, 2012. https://www.accuweather.com/en/weather-news/what-is-the-dense-fog-advisory/223402
[51] "FLIR BTS Sees Through a Smoke Grenade" YouTube video, October 18, 2012, 1:12, https://www.youtube.com/watch?v=sE6lBpwLc14
[52] https://www.researchgate.net/figure/Range-of-the-transmission-of-the-IR-spectra-ground-atmospheric-windows-25_fig5_299340479
[53] A Design for Maintaining Maritime Superiority 2.0. Department of Defense. December 2018. 10.
[54] Torrey Pines Logic AN-PAQ-6 datasheet. https://tplogic.com/an-paq-6/
[55] https://www.gsaadvantage.gov/advantage/s/search.do?q=0:2tfoca+ii+cable&db=0&searchType=0. Accessed January 22, 2019.
[56] http://www.fiberopticshare.com/single-mode-fiber-vs-multimode-fiber-choose-2.html.
[57] http://www.tfoca-tactical-fiber.com/PDF-Catalogs/Cables%20Plus%20USA%20FIBER%20OPTIC%20REELS%20Complete.pdf. 3.
[58] http://www.tfoca-tactical-fiber.com/PDF-Catalogs/Cables%20Plus%20USA%20FIBER%20OPTIC%20REELS%20Complete.pdf. 3.
[59] https://store.cablesplususa.com/ipramtas12fi1.html.
[60] https://www.nasa.gov/directorates/heo/scan/engineering/technology/txt_opticalcomm.html.
[61] Gen David Berger. Notes On Designing The Marine Corps Of The Future. https://warontherocks.com/2019/12/notes-on-designing-the-marine-corps-of-the-future/.
[62] Sydney J. Freedberg Jr. Marines Need Submarines: Commandant Neller On Major War. https://breakingdefense.com/2018/02/marines-need-submarines-commandant-neller-on-major-war/
[63] Joint Operating Environment 2035: The Joint Force in a Contested and Disordered World. Department of Defense. July 14, 2016. 17.