

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.						
1. REPORT DATE (DD-MM-YYYY) 29-03-2021		2. REPORT TYPE Master of Military Studies (MMS) thesis			3. DATES COVERED (From - To) AY 2020-2021	
4. TITLE AND SUBTITLE Keeping Quiet: How to Maintain a Kill Chain in a Communications Contested Environment				5a. CONTRACT NUMBER N/A		
				5b. GRANT NUMBER N/A		
				5c. PROGRAM ELEMENT NUMBER N/A		
6. AUTHOR(S) Gorsetbakk, Mikkel (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 US has shifted the main focus of its security strategy from counter-terrorism towards great power competition. US forces are currently revising their force design to adapt to these changes. USMC, specifically, is heading towards closer integration with the Navy and is developing Marine Littoral Regiments that will complement the Expeditionary Advanced Base Operation concept. This concept entails small, dispersed units to operate within the adversary's weapons engagements zone, thus making the units subject to the risk of detection and countermeasures. Sensors and shooters need to communicate to be effective, but China and Russia both have considerable capability and capacity within Electronic Warfare and Signals Intelligence in all domains that can detect and localize electromagnetic emissions. There are several different technologies available for beyond-line-of-sight communications, each with its strengths and weaknesses. USMC forces operating in a communications contested environment have to combine these technologies and rethink how they are being used and adjust and tailor communications procedures to minimize the chance of being compromised by their communications. The USMC should adjust its communications concept for EABO in the direction of an extended network of broadcasting stations, combined with communications systems designed to blend in with prominent civilian communication in the theater. Communication plans and Emission Control procedures will have to be tailored to meet the specific threat and signal environment of the operating environment. Dispersion of forces and long periods without two-way communications also requires military leaders to emphasize building independent Marines and units that can operate autonomously based on intentions rather than directions.						
15. SUBJECT TERMS Communications, PACE, EMCON, EW, SIGINT, LPI, LPD, HF, SATCOM, EABO, MLR, Communications Contested Environment, WES,						
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

TITLE:

**Keeping Quiet: How to Maintain a Kill Chain in a Communications
Contested Environment**

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

AUTHOR:

Major Mikkel Gorsetbakk, Norwegian Army

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member:

Craig A. Swanson PhD
Approved: [Signature]
Date: April 15, 2021

MMS Mentor Team and Oral Defense Committee Member:

LT Col Brian A. Woodward, USMC
Approved: [Signature]
Date: 15 APR 2021

*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

TITLE:

**Keeping Quiet: How to Maintain a Kill Chain in a Communications
Contested Environment**

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

AUTHOR:

Major Mikkel Gorsetbakk, Norwegian Army

AY 2020-21

MMS Mentor Team and Oral Defense Committee Member:

Approved: _____

Date: _____

MMS Mentor Team and Oral Defense Committee Member:

Approved: _____

Date: _____

Executive Summary

Title: Keeping Quiet: How to Maintain a Kill Chain in a Communications Contested Environment

Author: Major Mikkel Gorsetbakk, Norwegian Army

Thesis: By alternating between electromagnetic and non-electromagnetic communications systems, adapting the use of currently fielded systems, and changing communications procedures, it is possible to be silent when needed and to achieve a low probability of intercept (LPI) and low probability of detection (LPD) when transmissions are necessary.

Discussion: The US has shifted the main focus of its security strategy from counter-terrorism towards great power competition. US forces are currently revising their force design to adapt to these changes. The USMC, specifically, is heading towards closer integration with the Navy and is developing Marine Littoral Regiments that will complement the Expeditionary Advanced Base Operation concept. This concept entails small, dispersed units operating within the adversary's weapons engagements zone, thus making the units subject to the risk of detection and countermeasures. Sensors and shooters need to communicate to be effective, but China and Russia both have considerable capability and capacity within Electronic Warfare and Signals Intelligence in all domains that can detect and localize electromagnetic emissions. There are several different technologies available for beyond-line-of-sight communications, each with its strengths and weaknesses. USMC forces operating in a communications contested environment have to combine these technologies and rethink how they are being used, and tailor communications procedures to minimize the chance of being compromised by their communications.

Conclusion: The USMC should adjust its communications concept for EABO in the direction of an extended network of broadcasting stations, combined with communications systems designed to blend in with prominent civilian communication in the theater. Communication

plans and Emission Control procedures will have to be tailored to meet the specific threat and signal environment of the operating environment. Dispersion of forces and long periods without two-way communications also requires military leaders to emphasize building independent Marines and units that can operate autonomously based on intentions rather than directions.

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.

QUOTATION FROM, ABSTRACTION FROM, OR REPRODUCTION OF ALL OR ANY PART OF THIS DOCUMENT IS PERMITTED PROVIDED PROPER ACKNOWLEDGEMENT IS MADE.

Illustrations

Page

Figure 1: UHF SATCOM Coverage	9
-------------------------------------	---

Table of Contents

	Page
DISCLAIMER	iv
ILLUSTRATIONS.....	v
PREFACE	vii
INTRODUCTION.....	1
FORCE DESIGN	2
THREATS.....	3
COMMUNICATIONS TECHNOLOGY	6
PROCEDURES.....	12
LEADERSHIP	14
NARRATIVE.....	15
CONCLUSION	19
BIBLIOGRAPHY	25

Preface

When I selected this topic for my theses, it was more than anything else because someone told me to write about something that really interested me. The challenge of communications facing a peer or near-peer adversary is a topic that many have opinions on and talk about, but the subject is nevertheless somewhat understudied. I knew that writing about this topic would be challenging, as unclassified sources regarding Electronic Warfare and Signals Intelligence capabilities are hard to find. When I nevertheless chose to do so, it was to write something that hopefully would be a useful input for those who do not have access to classified content. Papers on this topic tend to be rather technical, which is why, in an attempt to make it more accessible to non-communicators, I have included a narrative in this paper.

I want to extend my gratitude to Dr. Craig Swanson and LtCol. Barian Woodward for coaching me through this process, as well as Dr. and Cdr. Stephen Kelley for his support and advice.

I was writing this thesis while attending the USMC Command and Staff College. Anyone that has done that knows that it takes quite a lot of time and effort, which is why I also have to thank my wonderful wife and my sons for providing support and patience on this journey.

"Tomorrow's fights will involve conditions in which 'to be detected is to be targeted is to be killed.' Adversaries will routinely net together sensors, spies, UAS, and space imagery to form sophisticated "ISR-strike systems" that are able to locate, track, target, and attack an opposing force. [...] No matter the means of detection, unmanaged signatures will increasingly become a critical vulnerability [...]. Defensively, our units will need to adapt how they fight, emphasizing emissions control and other means of signature management to increase their survivability."¹

INTRODUCTION

The US armed forces face immense upheavals from the strategical level, through the operational level, all the way down to the tactical and sub-tactical level. After some 20 years with a primary focus on fighting insurgents and chasing terrorists in the Middle East, the pendulum has now shifted towards great power competition with the main focus towards Indo-Asia-Pacific.² The shift has been relatively sudden and is well anchored and articulated on the USA's strategical level, including the 2017 National Security Strategy (NSS) that puts the Indo-Pacific with an increasingly competitive China on top of its list of regions of interest.³ In terms of great powers, the NSS states that "China and Russia challenge American power, influence, and interests, attempting to erode American security and prosperity."⁴ The new administration's Interim National Security Strategic Guidance from March 2021 agrees with the former administration's NSS, describing a China and Russia that "have invested heavily in efforts meant to check US strengths and prevent us from defending our interests and allies around the world."⁵ In the last 20 years, the US and its allies have fought their conflicts with few or no threats from electronic warfare or signals intelligence. Communication concepts developed through this period are not suitable for use within the range of peer or near-peer opponents' sensors and effectors. In this new orientation, the US

Marine Corps seeks closer integration with US Navy, emphasizing dispersed forward sensors and weapons deployed within the adversary's weapons engagement zone (WEZ). The question then becomes: how can the USMC maintain its kill chain while remaining hidden from an adversary with considerable resources within electronic warfare and signals intelligence?

This is a difficult question to answer: there are no magic boxes that will solve the issue of communicating safely in a communications contested environment. By alternating between electromagnetic and non-electromagnetic communications systems, adapting the use of currently fielded systems, and changing communications procedures, it is, however, possible to be silent when needed and to achieve a low probability of intercept (LPI) and low probability of detection (LPD) when transmissions are necessary.

FORCE DESIGN

The Department of the Navy has answered the new National Security Strategy with a concept for "naval operations in the littoral environment in light of emerging threats," underlining the need to increase the integration of the US Navy and US Marine Corps and examine "options for integrated Navy-Marine Corps operations to overcome sea denial forces in contested littoral environments."⁶ This concept argues the need for distributed lethality by dispersed forward sensors and weapons explicitly but simultaneously highlights the need for capabilities to "operate in a communication contested / degraded environment."⁷

The US Marine Corps immediately followed suit, with the Commandant of the Marine Corps in his planning guidance echoing the need for closer integration with the Navy, operations in littoral waters in a contested environment, and a drive for new force design towards a refinement of the Expeditionary Advanced Base Operations (EABO) concept from the 2016 Marine Corps Operating Concept.⁸ Commandant of the Marine Corps Gen. Berger kept his promise and followed up his planning guidance with his Force Design 2030, where

the construct of a Marine Littoral Regiment surfaces, along with an emphasis on the need for low signature of future units.⁹ The Department of the Navy's latest refinement to Force Design 2030 so far came in March 2021, in the form of a Tentative Manual for Expeditionary Advanced Base Operation (TM EABO). TM EABO states that "EABO will be conducted in an EMOE [electromagnetic operating environment] that is constrained, congested, and contested. Throughout the competition continuum, littoral forces will conduct EABO with denied, degraded, or disrupted access to the EMS [electromagnetic spectrum]."¹⁰ Further, it prescribes that "[l]ittoral forces must employ systems with small physical footprints capable of low-signature emanations, especially in cyberspace and across the electromagnetic spectrum (EMS) to neutralize or delay the adversary's targeting cycle, thereby creating a time advantage relative to the adversary."¹¹ The USMC is already on its way to establishing a Marine Littoral Regiment as part of the concept development and is currently testing the Norwegian Naval Strike Missile from land-based remote vehicles as part of the new force design.¹² Although a lot of the current focus is pointed towards the South China Sea and the First island chain in the western Pacific, Gen. Berger has also suggested that USMC might have a role in anti-submarine warfare (ASW) in the High North, relying on the same concept of dispersed forces acting as sensors and shooters.¹³ All in all, the need for distributed units with low signature, providing sensor coverage, and lethality is quite stringent and well documented.

THREATS

A detailed picture of the threat towards the electromagnetic signature is a little harder to find. Although official threat assessments, strategies, and concepts often include warnings about a contested electromagnetic spectrum, they mostly omit these capabilities' nature and threat.¹⁴ This lack of detail is probably due to the subject's sensitivity, and most sources will

likely be classified. Still, by piecing together information from different sources, it is possible to put together some usable assumptions.

The US Intelligence Community states in its Worldwide Threat Assessment from 2019 that both China and Russia continue to develop their ability to fight in all military domains. One has to assume that this also includes finding and negatively influencing actors in the electromagnetic spectrum.¹⁵ The Swedish Defence Research Agency offers a far more detailed picture of at least Russian capabilities and the organization's current status and development in one of their reports. The report expands very well on Russian doctrine, organization, development, and systems but does not reveal details like effect or frequency bands.¹⁶ Russia has invested heavily in SIGINT and Electronic Warfare (EW) systems for the past decades, partly as a "means of bridging technology gaps with the USA and other NATO member states, in the context of the generally deteriorating relationship between Russia and the West."¹⁷ Since 2010, more than 20 new EW complexes have completed Russian state trials, including ground, air, and naval systems.¹⁸ These new systems are produced in large numbers and fielded to an increasing number of EW units. As an example, Russia's more than 40 ground force major formations each reportedly have their own EW Company, in addition to the five independent EW brigades, generally subordinate to the Joint Strategic Commands.¹⁹ Another report from RAND Corporation echoes this perception. It paints a broader overview of Russian budgets and capabilities than the Swedish report but portrays Electronic Warfare as a field where Russia has high- capability and capacity.²⁰

Although specific details about Russian systems are hard to find in the unclassified realm, their systems' effects have been experienced in detail, much due to the conflict in Ukraine starting in 2014. The Organization for Security and Co-operation in Europe's (OSCE) Special Monitoring Mission (SSM) to Ukraine has reported observations of Russian Electronic warfare systems as well as having their drones affected by probable jamming.²¹

Ukrainian forces themselves also report loss of multiple drones due to "attacks on navigation systems through a tactic known as GPS spoofing," detection and jamming of counter artillery batteries, and suppression of radio communications. Russian drones with receivers and direction-finding capabilities are also reported, along with applied capabilities for jamming and exploiting GSM systems.²²

Finding details about China's capacities and capabilities within the electromagnetic spectrum is harder, presumably in part because China has not been part of any conflict of the same level as the conflict in Ukraine. When sifting through Janes' comprehensive records, one can nevertheless find small nuggets of information to start getting some form of an impression of the situation. The KJ-200B aircraft is reported to have antennas for electronic warfare and electronic support measures, and the ZDK-03, although an export version customized for Pakistan, is ELINT and COMINT capable.²³ This report also mentions a SIGINT aircraft called Y-9JB that has also been reported intercepted by Japanese fighter jets near Okinawa.²⁴ China is also exploring the segment of unmanned aircraft. Its newly developed UAV WJ-700 can allegedly carry both SIGINT and electronic warfare payloads and is a "maritime-oriented long-endurance system that can monitor vast coastlines or territorial waters, and if necessary be tasked to persecute threats on its own."²⁵ Another domain that can be utilized for intercept and detection is space. Although China does not reveal much information about its satellite payload, unclassified sources have indicated that the Yaogan-satellites 9, 16, 17, 20, 25, and 30 launched between 2010 and 2018 have an ELINT/SIGINT payload and can detect and geolocate electromagnetic emitters in oceanic environments.²⁶

Specific information on electronic warfare, SIGINT, and ELINT capabilities are kept under a tight lid by most actors. The same goes for what they know about other actors' capabilities in order to guard their intelligence capabilities. Nevertheless, based on unclassified findings, it seems fair to assume that a conflict with a peer or near-peer opponent

will involve a threat to the use of communications systems. Beyond line of sight (BLOS) communications carries with it the inherent trait of long-range electromagnetic emissions that are vulnerable to detection and intended interference. With both China and Russia investing heavily in electronic warfare, SIGINT, and ELINT capabilities on land and sea, and in air and space, one has to assume that all BLOS transmissions imply the risk of detection and geolocalization.

COMMUNICATIONS TECHNOLOGY

With threats of possibly being detected and geolocalized in the electromagnetic spectrum, the US forces have a job to do, both in terms of technology but not least in concepts and procedures. A report from the Center for Strategic and Budgetary Assessments (CSBA) claims that "Since the Cold War, US forces have operated with little regard for enemy SIGINT and ELINT satellites, aircraft, and ground sensors. Even if an enemy had sensors that could detect RF emissions, US forces assumed they would not be capable of geolocating the source of the signals with quality targeting accuracy".²⁷ The same report urges for more active use of emission control (EMCON) combined with the application of communications systems with Low Probability of Intercept (LPI) and Low Probability of Detection (LPD), and also offers some examples for such systems. Mission-type orders with intent-based objectives and pre-plan de-confliction are good advice to remove the need for communication between units. Still, with more extended periods of operation and changing rules of engagement, that will not always be possible. Although offering some excellent thoughts on the subject, the report does not provide sufficient depth and detail to conceptualize a realistic communication concept for dispersed forces in a communications contested environment.²⁸

The report from CSBA refers to two specific technologies for LPI/LPD: High Frequency (HF) radio and Troposcatters.²⁹ The HF frequency band has radio waves that refract in the earth's ionosphere, thus enabling it to be used for long-distance Beyond Line of

Sight (BLOS) communication without the need for intermediate infrastructure like, for example, satellite communication. Transmissions can, in theory, travel around the globe but vary in practice a lot depending on conditions in the ionosphere. This makes HF transmitters vulnerable for detection and geolocalization. HF radio waves are, on the other hand, challenging to direct precisely, making it very hard for an adversary to predict the desired geographical impact of the signal, provided that the receiver does not emit anything in response. HF is not traditionally known to be neither easy to operate nor reliable for continuous communications. The frequency range of HF, spanning from 3MHz to 30MHz, requires large antennas as HF wavelengths span from 10 to 100 meters. Tactical antennas often size between 50 and 75 meters in the horizontal plane but are typically wire-based and offer low weight and volume for transportation.³⁰

The low bandwidth available in the HF frequency band also offers relatively low data throughput compared to higher frequency bands. Still, a study on new 4th generation HF radio has shown that continuous connection can be expected through self-adaption to channel conditions, with an average data throughput between 10 kb/s and 50 kb/s.³¹ That sort of throughput will realistically provide transfer of text and small pictures but will not support more demanding transmissions like video. Currently fielded tactical HF radios have built-in options for *receive-only*, which means that the radio can remain idle receiving voice and data transmissions without transmitting any signals.³²

Troposcatters, short for tropospheric scatters, have some of the same characteristics as HF but rely on much higher frequencies, around 2 GHz, where radio-waves bounce in the tropopause between the earth's troposphere and stratosphere before heading back to earth. Troposcatters offer much higher bandwidth than HF but cannot be used for as long distances, capable of a maximum distance of approximately 200 miles.³³ As an example, the AN/TCS-198 (V3) has been claimed to have "established and maintained a 50-Mb/s troposcatter

communication link in excess of 100 miles", surpassing HF throughput by a thousand times.³⁴

Besides range, antennas are also a limiting factor for troposcatters as large, heavy; parabolic antennas are needed to direct the energy sufficiently. Broadcasting is not a feature typically used with troposcatters but would probably be feasible.

Tactical UHF satellite communication, or UHF SATCOM, has seen widespread use by US forces since the first UHF Follow-on (UFO) satellite was launched in 1993. The frequency band (290–320 MHz uplink and 240–270 MHz downlink) offers the ability to "penetrate foliage and atmospheric conditions such as clouds, rain, or fog," as well as small, low-weight antennas that do not demand painstaking precision when establishing a connection.³⁵ Data throughput is up to 64 kb/s, offering more speed than HF but much less than troposcatters. UHF SATCOM utilizes geosynchronous satellites with antennas transmitting to an extremely wide area, making it impossible to predict the desired geographical impact of the signal based on the signal from the satellite and like with tactical HF radios, currently fielded UHF SATCOM terminals has built-in features that allow a station to remain silent in *receive-only*.³⁶ This means that one or more transmitting stations within the same satellite coverage as the receiving station(s) can broadcast voice or data continuously if needed, without exposing the receiving station(s) to SIGINT detection or detection-finding. A UFO satellite coverage area will typically be approximately 140° in longitude and $\pm 70^\circ$ in latitude, allowing for, for example, a transmitting station in Eastern Europe and a receiving station in Australia, see Figure 1: UHF SATCOM Coverage. With its simplicity of operations, stable communications, and a large number of fielded radios, UHF SATCOM provides a very

favorable option for broadcast operations.

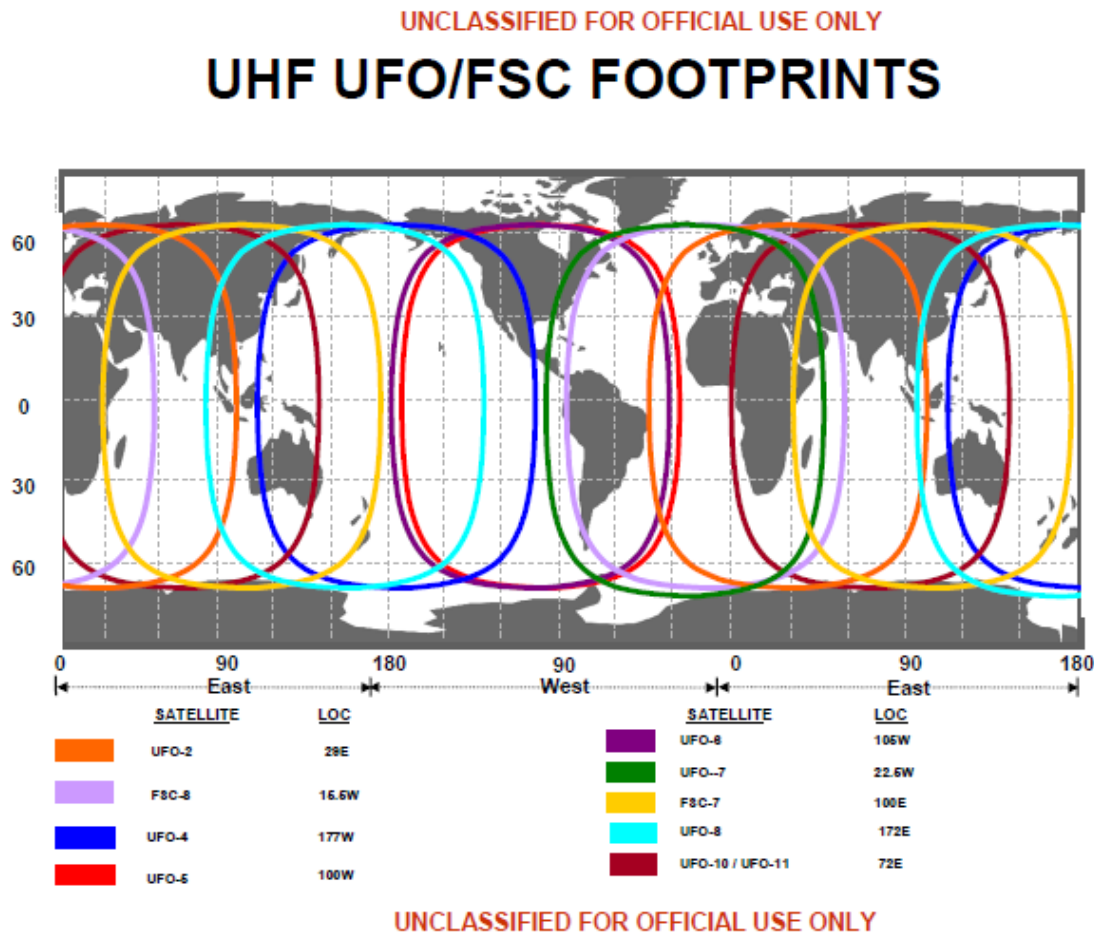


Figure 1: UHF SATCOM Coverage

Source: Naval Network Warfare Command. Naval Telecommunications Procedures - NTP 4 (E). Norfolk, V.A.: Naval Network Warfare Command, 2008. 5-19.

In addition to UHF SATCOM, there are a number of different providers of satellite communication, and the number of different solutions is increasing. Most civilian SATCOM solutions utilize much higher frequencies than UHF SATCOM, with both positive and negative effects. On the positive side, higher frequencies typically offer larger bandwidth, which entails higher data throughput and more services accordingly. On the other side, higher frequencies entail higher attenuation of the signal traveling between the satellite and ground, demanding more advanced antennas and terminals that need very accurate pointing to establish and maintain a connection. Higher frequencies are also more vulnerable to physical obstacles like foliage and, to a certain degree, rain, snow, and fog. Because of the more

advanced nature of these SATCOM services, ground terminals typically also have to communicate with the satellite to establish and maintain a condition, depriving them of the option of remaining in radio silence. On the other side, with 30 000 vessels using very small aperture terminals (VSAT) throughout the world in 2018, the possibility to disappear in the crowd is much more prominent when using civilian satellite services.³⁷ Some providers offer simple messaging systems via satellite, where data-bursts are transmitted from the satellite over a large geographic area. Some of these satellite pagers have built-in *receive-only* functionality, making them impossible to detect through SIGINT or Electronic Warfare capabilities.³⁸ Satellite pagers like this can serve as a valuable addition to a communications plan due to their small form-factor, low power consumption, and electromagnetic stealth capabilities.

Communication through commercial low earth orbit (LEO) satellites is a new technology currently not fully operational but will most likely be in just a few years. Several companies have launched satellites and are performing trials, for example, Starlink with more than 1000 satellites already in space and OneWeb with 110 satellites.³⁹ With its large number of satellites and its relatively low distance to earth, LEO constellations can offer high data throughput and low signal latency. With currently fielded technology, "users can expect data speeds from 50Mbps to 150Mbps, with latency in the range of 20-40ms in most locations," dramatically surpassing the performance of HF, UHF SATCOM, and VSAT terminals.⁴⁰ Whether this technology is suitable for broadcasting services is yet unclear, but as the number of users increases, it might provide an opportunity to blend in with commercial traffic.

The internet is the planet's highway for information-exchange and is available in some form in most, if not all, places on earth. As of 2019, the number of internet users passed 4 billion, more than half of the earth's population.⁴¹ When discussing the internet for communications, it is imperative to distinguish between the internet itself and the

communication carrier that connects the user to it. Examples of such carriers are cabled modems, mobile phones, and satellite terminals, and will not be discussed in this section. Due to the prevalence and the excessive number of internet users, it is more feasible to hide one's activity using it compared to communicating through electromagnetic emissions, especially in the military frequency bands where the number of users is relatively limited. It is also feasible to maintain the confidentiality of the information through different military and commercial methods. There are several government off-the-shelf (GOTS) approved encryption methods that can be used to transport classified content through the internet, for example, the High Assurance Internet Protocol Encryptor (HAiPE), either alone or in concert with commercial off-the-shelf (COTS) products.⁴² Utilization of the abundance of COTS products available for internet information confidentiality has two major benefits. If only COTS products are used, one is that regulations for transport and storage of COTS equipment are often less strict than for Controlled Cryptographic Items (CCI) that are often needed for GOTS encryption. Another benefit is that COTS products are more widely used, thus making it harder to identify as military traffic should the transmission be detected. COTS products do not have the same level of resilience and control as GOTS products and will normally not be approved for classified information. However, a layered combination of certified components has been approved by the National Security Agency (NSA) in a program called Commercial Solutions for Classified (CSfC), "founded on the principle that properly configured, layered solutions can provide adequate protection of classified data in a variety of different applications."⁴³ Internet prevalence and usage will most certainly continue to expand in the future and provide information confidentiality and a high degree of protection against detection if utilized thoughtfully.

PROCEDURES

A vital part of a communications plan is the PACE-plan, which states Primary, Secondary, Contingency, and Emergency means of communications. A PACE plan has to be tailored to the specific unit, the specific mission, and can also change through different phases of a mission. The different elements in the PACE plan should incorporate different means of communication, as well as how one should use them. For example, to use different frequencies or different radio modes for the same tactical radio set as primary and secondary means of communication is useless if the radio set itself breaks down.

Another factor in communications planning is Emission Control (EMCON). JP 3-85 Joint Electromagnetic Spectrum Operations defines EMCON as "The selective and controlled use of electromagnetic, acoustic, or other emitters to optimize command and control capabilities while minimizing, for operations security: a. detection by enemy sensors, b. mutual interference among friendly systems, and/or c. enemy interference with the ability to execute a military deception plan."⁴⁴ The US Navy has four primary levels of EMCON that can be adjusted as needed, where EMCON Delta is the lowest level where emissions are unrestricted, EMCON Charlie "can be used to disguise a specific unit by de-energizing emitters to a particular platform," EMCON Bravo adds more restrictions but still allows for certain critical communications, and EMCON Alfa is generally complete silence with no permitted emissions.⁴⁵ Combining a PACE plan and an EMCON plan gives the commander a powerful tool to adjust the use of communications adapted to the specific threat at any given time.

Primary means of communication for dispersed units operating in a communications contested environment should be *receive-only*, or EMCON Alfa, listening to broadcasts from UHF SATCOM, HF, troposcatter, or commercial SATCOM. The node will be able to receive situation updates, new tasking, and changes to PACE and EMCON procedures in this state.

Changes to EMCON procedures could include what procedure to follow if electromagnetic signals have been emitted, based on the enemy situation, e.g., stay in position, move to a new location, or start extraction. The node will not be emitting any intended electromagnetic waves in EMCON Alfa and will remain undetectable in the electromagnetic spectrum.

Secondary means of communication to stay undetected should be through a non-emitting connection to the internet, with the information secured by GOTS or COTS security mechanisms and masked by using a commonly used COTS product. If regular cabled internet is not available at the node's location, a tactical wired connection could be established with metal or fiber optic cable if deemed feasible by the tactical situation. The node would not emit any intended electromagnetic waves detectable by electronic warfare, SIGINT, or ELINT capabilities. Still, one has to make assumptions on the risk of being detected through internet surveillance based on geography and the adversary.

Contingency means of communication should be to blend electromagnetic transmissions in with civilian traffic to the greatest extent. The Intelligence Preparation of the Battlefield (IPB) must include surveys of the standard signal environment in the area and guide technology choice. While a commonly used SATCOM terminal could be the best solution in a rural, coastal environment with heavy ship-traffic, a locally bought mobile phone with an internet access point could be a more challenging target to detect in an urban setting. A unit can also move the prescribed communications equipment to a different area before making the connection, deceiving a potential adversary's detection of the node's specific location. Again, subject matter experts will have to make continuous threat assessments and update the node on what actions to take after transmitting electromagnetic energy.

Emergency means of communication will often be by any means possible. In this case, the last resort will often be communications equipment with obvious military signature, like UHF SATCOM, HF radio, or Troposcatter. Although one can still maintain the confidentiality

and integrity of the information by encryption, an adversary with peer or near-peer capabilities could detect the node's presence and location. Still, even if one assesses that the transmission is detected and geolocalized, the adversary's will and ability to take actions against the node have to be considered before directing the action the node should take after transmitting.

LEADERSHIP

After the successful raid killing Osama Bin Laden on May 2 in 2011, a picture by Pete Souza has become almost as famous as the raid itself: the picture of President Obama and other US officials in the White House Situation Room, watching in suspense the live feed from the compound in Abbottabad, Pakistan. Although this was a very special and unique operation, it paints a picture of the ability to watch military operations play out on the screen, in real-time from literally anywhere in the world. From operations in Afghanistan and Iraq, commanders and their staff have grown accustomed to seeing the result from their planning unfold through full-motion video captured by ISR platforms overhead. Likewise habitual is the battle wheel, with its Commanders Update Brief (CUB), which feeds, among other things, from the daily situation reports received from all units in the field. Cyclical communication checks to all units are yet another control mechanism that most military professionals have grown accustomed to. These examples are all something that most likely will have to disappear in a peer or near-peer conflict in a communications contested environment. Even though this represents a change in procedures and habits developed during the last decades of counterinsurgency operations, it does not conflict with the USMC's philosophy of command. In its chapter Philosophy of Command, MCDP-1 Warfighting states that "subordinate commanders must make decisions on their own initiative, based on their understanding of their senior's intent, rather than passing information up the chain of command and waiting for the decision to be passed down. Further, a competent subordinate commander who is at the

point of decision will naturally better appreciate the true situation than a senior commander some distance removed."⁴⁶ The change in force design, tactics, and reporting procedures should thus not require a change in command philosophy, rather a revitalization of the existing one.

NARRATIVE

The narrative in this section aims to connect the previous sections by placing force design, threats, communications technology, procedures, and leadership into a fictive scenario. It portrays different functions of a future USMC unit in a littoral environment in a conflict where US forces are working to establish sea denial. The narrative demonstrates how communication can flow between sensors, leadership, and shooters, with procedures and communications technology adapted to the threat in the area of operations.

The reconnaissance team had been working from their position for more than a week. Since they haven't had anything to report this far, they had been able to maintain absolute radio silence without any electromagnetic emissions. Except for a few short periods, possibly due to jamming, they had constantly been receiving updates on the situation, intelligence from other assets, and changes in EMCON state from higher. The latest update from the UHF SATCOM broadcast was that the threat-assessment in that area allowed for reporting, if needed, performed through covert internet usage as long as nothing was transmitted through the air. The team's small unmanned surface vessel (USV) returned earlier than planned from its pre-programmed search pattern, and its diagnostics reported that it had lost GPS signal, triggering it to backtrack and return home. A quick scan of the recorded sensor-data revealed the probable cause of loss of GPS signal: the USV had discovered a hostile ship formation and had most likely had its GPS signals jammed. The USV had nevertheless been able to use its sensors and could reveal the speed, heading, and composition of the formation, as well as a few good signature patterns that could prove invaluable if added to the recognition library of

the anti-ship missiles (ASM). Not long after, part of the team had moved to their safe-house and was uploading the encrypted military data, tunneled through a commercial encryption tunnel, to higher via the internet land-line. With the threat-integration for the selected reporting method deemed LOW through EMCON-state, the team finished up in the safe-house and continued their mission.

The commander was sitting in the back of the room, quietly observing the tactical operations center that was, as always, buzzing with activity. It was uncomfortable to have so many units dispersed out through the area of operations (AO) with little or no reporting on their status. Still, the commander knew that the Marines were well trained and equipped to handle both expected and unexpected challenges. The intelligence cell was monitoring the adversary situation in the area of interest (AOI) continuously, both through its own collection assets and other received reporting, turning it into assessments for the staff and the units in the field. They had just received NSA reporting that one of the virtual private network (VPN) providers from the CSfC white-list had been moved to the black-list due to a security breach, but the communications cell confirmed that no units were actually using that VPN in their systems. Information about the compromised VPN would still be incorporated in the situation updates that the TOC pushed continuously to the field units through several different communications systems and from several sites, both locally and remotely operated as far away as other continents. The report on the hostile ship formation from the reconnaissance team provided the last piece of a puzzle the intelligence cell had been working on for a while. Other sensors had already detected the formation and were tracking it, but the fidelity of the sensors was not good enough to positively identify the ships. Now, with the data from the USV, they had all they needed to engage the formation. The TOC immediately transmitted a satellite pager message, directing all units to monitor broadcasts continuously. After calculating when the hostile formation would enter the pre-planned engagement area, the

TOC could distribute warning orders for the weapons-teams and orders for both the BDA-teams and the exfiltration-assets. While the field units prepared, the TOC would continue tracking the formation before sending updated signature profiles for the missiles along with the final fire-mission as soon as the formation entered the engagement area.

The weapons-team was idle and had been for quite a few days. They were now well into routine operations after infiltrating into position with their anti-ship missile launcher and thoroughly camouflaging it. Like the reconnaissance team, they would tap into the broadcast to get updates at specific intervals, but recently the EMCON state had changed through a satellite pager message, directing the team to monitor the broadcast continuously. The daily proof of life message to higher had been a welcomed break in the routine for the team, as they would send two Marines to the outskirts of a small town in the area to send a message through a locally purchased cellphone. Although the widely used app they utilized for sending the message, in theory, could be intercepted and decrypted, it would not reveal anything more than a random everyday sentence in the local language that served as the team's code-word for "everything ok." When the team received their fire-mission over UHF SATCOM, everything happened very fast. While two Marines uploaded the target data and the updated target signature for the recognition library to the missiles, other team members made sure their VSAT terminal was ready to be activated. At the prescribed time before launch, they connected the VSAT. They confirmed to HQ that they were prepared for launch on the encrypted link, knowing that enemy intelligence would use a considerable time to distinguish their terminal from all the other VSAT traffic in the area if at all able to do that. If the terminal were detected, the information would still be secure, and locating the signal would be even more difficult than detecting it in the short time-span they were active. Immediately after sending their "launch successful" message, they withdrew from their position and moved to their pre-planned secondary launch position to be ready for a potential re-attack.

A second reconnaissance team's mission had been a rough one. The team's infiltration had been wet and rigorous, unfortunately rendering their UHF SATCOM radio inoperable. Luckily, their HF radio was working fine, and with the dense vegetation around their position, they had no problem establishing the dipole-antenna. The ionospheric condition had in no way been optimal during their mission. However, with updates broadcasted on several different frequencies, they had still received messages several times a day, as the radio automatically scrolled through the presets listening for the best signal. As there were no internet land-lines in the area, they had to send their reports through their VSAT terminal, which they established when needed in a surveilled area some distance away from their observation post. When they were re-tasked to perform battle damage assessment (BDA), they quickly packed up and headed to their new position. This location would give them a visual line of sight to the target but would also make them more exposed. Anyway, they would not stay there for long. When the missiles hit the target, their VSAT terminal was already online, and after submitting an initial BDA-report, the team packed up and started their exfiltration. The same asset picking up the weapons-team would meet them at their rendezvous-point later.

As depicted in this narrative, there are ways to maintain situational awareness for sensors and shooters operating under severe threat from adversary EW and SIGINT capabilities. Forces outside the contested communications environment can feed units operating under threat with mission updates, intelligence, and procedures that minimize detection risks, using currently fielded communications technology. Well-trained and equipped Marines, comfortable with independent operations over time, can maintain electromagnetically undetected until they engage the adversary.

CONCLUSION

After more than two decades of fighting inferior technological adversaries, US forces are now facing a new reality. With growing competition with an increasingly powerful China and Russia testing out its new military arsenal in neighboring countries, the US assumption of full freedom of movement in the physical and electromagnetic domain is dead. With a vision of ensured American security and prosperity, US forces have shifted their focus towards the possibility of fighting a peer or near-peer adversary. The US Navy and USMC are revisiting their roots, seeking a closer integration in the realization that The US Navy might need some help to establish and maintain sea control, or even sea denial. Gen. Berger's Force Design 2030 for the USMC prescribes Marine Littoral Regiments and new capabilities that can threaten an adversary at sea from the shore. Dispersed forces operating from expeditionary advanced bases within the range of an adversary, advanced sensors and weapons are being developed and war-gamed. While the US was engaged in and focused on counter-terrorism, China and Russia have kept increasing and developing their respective arsenals. Their ability to deliver kinetic effects has increased in range and precision, as has their ability to detect and locate electromagnetic emissions. Ground, sea, air, and space-based platforms are now capable of detecting and locating almost any emission, as long as the sensors are queued to the specific area of the emission.

If USMC sensors and effectors are to be effective within reach of the adversaries' weapons and sensors, they would have to communicate in some form. When findings within the threats are compared to findings within the existing technology, it becomes apparent that there is no one solution that can solve the entire problem set, but rather a combination of different technologies, mixed with a set of adaptable procedures, that has to be developed. One of the greatest challenges with the threat from electronic warfare, SIGINT, and ELINT sensors is that there is no way of knowing whether one has been detected or not. The only

way of making sure that emissions are not detected is to not emit anything, actualizing the need to develop robust broadcasting systems that can continually update forces within a communications contested environment on the current threat and mission from secure locations. When the exposed units, at some point, have to communicate in order to fulfill their mission, they should do so according to a mission-specific PACE and EMCON plan, tailored to blend the communication to a maximum extent into the usual communications traffic environment of that specific area. The prescribed tool to communicate could be a cable internet connection, a civilian SATCOM terminal, or a mobile phone, all dependent on the signal environment and the adversaries' assumed capabilities. Key to the EMCON plan will be a threat integration of the adversaries' capabilities, both to detect the traffic and to engage in responsive actions, directing forces' operating procedures upon communicating.

This change is not merely limited to technology and procedures for tactical units and command posts; it will also have to involve a mental change within the military leadership. The frequent situational reports and the relaying of full-motion video back to the command post, a luxury one has grown accustomed to for the last decades, are just not compatible with operating in a communications contested environment. Leaders will have to trust that their men and women on the front line are capable of doing their job independently and of embracing the attitude that no news is good news.

This study has a narrow scope and is limited to unclassified sources and details within the possible solutions. Further studies could investigate robust technological solutions to optimize broadcasting techniques and techniques to mask military traffic within commercial communications solutions. Currently fielded and planned weapons systems with integrated communications solutions should be assessed and possibly redesigned or adjusted to allow for a radio-silence option. The communications concept recommended in this paper should be further refined through proof-of-concept trials to consider implications to training,

organization, planning considerations, and the other warfighting functions. Although this communications concept is aimed towards the EABO concept, its suitability should also be considered towards other operating concepts.

¹ Department of the Navy. *The Marine Corps Operating Concept - how an Expeditionary Force Operates in the 21st Century*. Washington, D.C.: Headquarters United States Marine Corps, September, 2016. 6.

² Jonathan Greenert, Joseph F. Dunford, and Paul F. Zukunft. *A Cooperative Strategy for 21st Century Seapower: Forward, Engaged, Ready*. (Washington, DC, 2015)

³ The White House. *National Security Strategy of the United States of America*. (Washington, DC, 2017). 45, 46.

⁴ The White House. *National Security Strategy of the United States of America*. (Washington, DC, 2017). 2.

⁵ The White House. *Renewing America's Advantages - Interim National Security Strategic Guidance*. Washington, D.C.: The White House, 2021. 8.

⁶ Department of the Navy. *Littoral Operations in a Contested Environment*. (Washington, DC, 2017). 3.

⁷ Department of the Navy. *Littoral Operations in a Contested Environment*. (Washington, DC, 2017). 18.

⁸ 38th Commandant of the Marine Corps. *38th Commandant's Planning Guidance 2019*. (Washington, DC, 2019). 9.

Department of the Navy. *The Marine Corps Operating Concept - how an Expeditionary Force Operates in the 21st Century*. Washington, D.C.: Headquarters United States Marine Corps, September, 2016. 13.

⁹ 38th Commandant of the Marine Corps. *Force Design 2030* (Washington, DC, 2020). 5, 12.

¹⁰ Department of The Navy. *Tentative Manual for Expeditionary Advanced Base Operations*. Washington D.C.: Headquarters, United States Marine Corps, 2021. 5-8.

¹¹ Department of The Navy. *Tentative Manual for Expeditionary Advanced Base Operations*. Washington D.C.: Headquarters, United States Marine Corps, 2021. 5-2.

¹² Globalsecurity.org. "Marine Littoral Regiment." Accessed February 20, 2021.
<https://www.globalsecurity.org/military/agency/usmc/mlr.htm>.

Mallory Shelbourne. "Marine Corps to Stand Up First Marine Littoral Regiment in FY 2022." Accessed Feb 20, 2021. <https://news.usni.org/2021/01/20/marine-corps-to-stand-up-first-marine-littoral-regiment-in-fy-2022>.

¹³ Berger, David. "Marines Will Help Fight Submarines." *U.S. Naval Institute Proceedings* 146, no. 11 (2020).

18-23. <https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=146687325&site=ehost-live>.

¹⁴ Joint Chiefs of Staff. *Joint Concept for Entry Operations*. (Washington, DC, 2014). 15.

¹⁵ Daniel R Coats, *Worldwide Threat Assessment of the US Intelligence Community Office of the Director of National Intelligence*, (Washington, DC, 2019). 26, 37.

¹⁶ Jonas Kjellén, *Russian Electronic Warfare - The Role of Electronic Warfare in the Russian Armed Forces*, Swedish Defence Research Agency, (Sweden, 2018).

¹⁷ Jonas Kjellén, *Russian Electronic Warfare - The Role of Electronic Warfare in the Russian Armed Forces*, Swedish Defence Research Agency, (Sweden, 2018). 13.

¹⁸ Jonas Kjellén, *Russian Electronic Warfare - The Role of Electronic Warfare in the Russian Armed Forces*, Swedish Defence Research Agency, (Sweden, 2018). 42-61.

¹⁹ Jonas Kjellén, *Russian Electronic Warfare - The Role of Electronic Warfare in the Russian Armed Forces*, Swedish Defence Research Agency, (Sweden, 2018). 36.

²⁰ Keith Crane, Olga Oliker, and Brian Nichiporuk. *Trends in Russia's Armed Forces*. The RAND Corporation, (Santa Monica, 2019). 65, [https://ebookcentral.proquest.com/lib/\[SITE_ID\]/detail.action?docID=6201997](https://ebookcentral.proquest.com/lib/[SITE_ID]/detail.action?docID=6201997).

²¹ Organization for Security and Co-operation in Europe. *Latest from OSCE Special Monitoring Mission (SMM) to Ukraine Based on Information Received as of 19:30 (Kyiv Time)*, (Kiev, August 16, 2015), <https://www.osce.org/ukraine-smm/177826>.

²² Makichuk, Dave. *Lessons Learned from the Battle of Ukraine*. Asia Times, (September 1, 2019). <https://asiatimes.com/2019/11/lessons-learned-from-the-battle-of-ukraine/>.

²³ Janes *C4ISR & Mission Systems: Air "C2 Facilities - Y8/Y9/Y20-Based AEW&C Aircraft"*. (November 18, 2020). <https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=FileName&ItemId=jaem0254&pubabbrev=jc4ia&Edition=2021>.

²⁴ Franz-Stefan Gady. "Japan Scrambles Fighter Jets to Intercept Chinese Y-9JB Aircraft Over East China Sea," *The Diplomat*. (18 December, 2018). <https://thediplomat.com/2018/12/japan-scrambles-fighter-jets-to-intercept-chinese-y-9jb-aircraft-over-east-china-sea/>.

²⁵ Kelvin Wong. "Image of New Chinese MALE/HALE UAV Emerges, Likely CASIC WJ-700 Prototype." *Jane's International Defence Review* (18 August, 2020). https://customer.janes.com/DefenceEquipment/Display/FG_3336007-IDR.

²⁶ *Jane's Space Systems and Industry*, "Space Systems - Yaogan Series." (9 May, 2019).

https://janes.ihs.com/CustomPages/Janes/DisplayPage.aspx?DocType=FileName&ItemId=jsd_a201&pubabbrev=jsd&Edition=2019.

²⁷ Bryan Clark, Mark Gunzinger, and Jesse Sloman. "Winning in the Gray Zone: Using Electronic Warfare to Regain Escalation Dominance." *States News Service*, (October 5, 2017). 59.

²⁸ Bryan Clark, Mark Gunzinger, and Jesse Sloman. "Winning in the Gray Zone: Using Electronic Warfare to Regain Escalation Dominance," *States News Service*, (October 5, 2017). 60.

[https://csbaonline.org/uploads/documents/CSBA6305_\(EMS2_Report\)Final7-web.pdf](https://csbaonline.org/uploads/documents/CSBA6305_(EMS2_Report)Final7-web.pdf).

²⁹ Bryan Clark, Mark Gunzinger, and Jesse Sloman. "Winning in the Gray Zone: Using Electronic Warfare to Regain Escalation Dominance." *States News Service*, (October 5, 2017). 61.

[https://csbaonline.org/uploads/documents/CSBA6305_\(EMS2_Report\)Final7-web.pdf](https://csbaonline.org/uploads/documents/CSBA6305_(EMS2_Report)Final7-web.pdf).

³⁰ L3Harris Technologies, Inc. *RF-1941/RF-1940 SERIES DF Manpack, Portable Dipole Antenna*. Melbourne, F.L: L3Harris Technologies, Inc., 2020.

³¹ Vivianne Jodalen and Terje Mikal Mjelde. *HF-Kommunikasjon i Arktis - Analyse Basert På Målinger*. Norwegian Defence Research Establishment (FFI), (Kjeller, Norway: 2016). 3-4.

³² Harris Corporation, RF Communications Division. *AN/PRC-150(C) Advanced Tactical HF Radio Operation Manual*. Rochester, N.Y: Harris Corporation, 2007. 3-18.

³³ John Keller, "Army Revisits Troposcatter Communications Technology as Alternative to Long-Range SATCOM," *Military and Aerospace Electronics*, (July 26, 2013). <https://www.militaryaerospace.com/rf-analog/article/16715796/army-revisits-troposcatter-communications-technology-as-alternative-to-longrange-satcom>.

³⁴ Iliza Sokol, "Troposcatter System Maintains 50-Mb/s Connection Over 100 Miles." *Microwaves&RF*, Accessed Feb 2, 2021. <https://www.mwrf.com/technologies/systems/article/21846099/troposcatter-system-maintains-50mbs-connection-over-100-miles>.

³⁵ D. A. Fritz et al., "Military Satellite Communications: Space-Based Communications for the Global Information Grid." *Johns Hopkins Apl Technical Digest* 27, no. 1 (2006). 34.

³⁶ Harris Corporation, RF Communications Division. *AN/PRC-117G Multiband Manpack Radio Reference Guide*. Rochester, N.Y: Harris Corporation, 2010.

³⁷ "The Complete Guide to Vsat 2019." *ISSUU*, Accessed Feb 7, 2021. https://issuu.com/rivieramaritimemedia/docs/vsat_2019_issuu.

³⁸ "GDB Pager." Accessed Feb 11, 2021. *Iridium*, <https://www.iridium.com/products/gdb-pager/>.

³⁹ Paul Lilly. "SpaceX Starlink Satellite Broadband Internet Preorders are Now Open to the Public." Accessed Feb 21, 2021. <https://hothardware.com/news/spacex-starlink-satellite-broadband-internet-preorders-open>.

OneWeb. "OneWeb's Successful Launch, Paves the Way for Commercial Services." Accessed Feb 21, 2021. <https://www.oneweb.world/media-center/onewebs-successful-launch-paves-the-way-for-commercial-services>.

⁴⁰ Paul Lilly. "SpaceX Starlink Satellite Broadband Internet Preorders are Now Open to the Public." Accessed Feb 21, 2021. <https://hothardware.com/news/spacex-starlink-satellite-broadband-internet-preorders-open>.

⁴¹ J. Clement. "Internet Usage Worldwide – Statistics & Facts." *Statista*, Accessed Feb 20, 2021. <https://www.statista.com/topics/1145/internet-usage-worldwide/>.

⁴² Committee on National Security Systems. "National Policy Governing the use of High Assurance Internet Protocol Encryptor (HAIPE) Products." *Cnssp* no. 1. June 19, 2013. [https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.361.5714&rep=rep1&type=pdf#:~:text=policy%20su,percedes%20CNSS%20Policy%2019,%20%E2%80%9CNational%20Policy%20Governing,the%20Federal%20Information%20Security%20Management%20Act%20\(FISMA\)%20of](https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.361.5714&rep=rep1&type=pdf#:~:text=policy%20su,percedes%20CNSS%20Policy%2019,%20%E2%80%9CNational%20Policy%20Governing,the%20Federal%20Information%20Security%20Management%20Act%20(FISMA)%20of).

⁴³ National Security Agency Central Security Service. "Commercial Solutions for Classified Program (CSfC)." Accessed February 20, 2021. <https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Trusted-Integrators/archived/>.

⁴⁴ Joint Chiefs of Staff. *Joint Electromagnetic Spectrum Operations* JP 3-85. Washington, D.C.: Joint Chiefs of Staff, 2019. GL-9.

⁴⁵ William D. Flanagan. *Flexibility in Decisive Action and Recommendations to Mitigate Risk: Electromagnetic Spectrum Footprint and Emissions Control* CEMA, AWG, PEO C3T, CACI, 2020.

⁴⁶ Department of the Navy. *MCDP 1 - Warfighting*. Washington, D.C.: Headquarters, United States Marine Corps, 1997. 78.

Bibliography

Berger, David. "Marines Will Help Fight Submarines." *U.S. Naval Institute Proceedings* 146, no. 11 (November, 2020): 18-23.

<https://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=146687325&site=ehost-live>.

Clark, Bryan, Mark Gunzinger, and Jesse Sloman. "Winning in the Gray Zone: Using Electronic Warfare to Regain Escalation Dominance" *National Defense (Washington)* 102, no. 770 (October 5, 2017)

Coats, Daniel R. *Worldwide Threat Assessment of the US Intelligence Community* Office of the Director of National Intelligence, January 29, 2019.

Commandant of the Marine Corps. *38th Commandant's Planning Guidance 2019*.

Washington, DC: Headquarters, United States Marine Corps, 2019.

Commandant of the Marine Corps. *Force Design 2030*. Washington, DC: Headquarters, United States Marine Corps, March 2020.

Committee on National Security Systems. "National Policy Governing the use of High Assurance Internet Protocol Encryptor (HAIPE) Products." *Cnssp* no. 19 (June 10, 2013).

[https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.361.5714&rep=rep1&type=pdf#:~:text=policy%20supersedes%20CNSS%20Policy%2019,%20%E2%80%9CNational%20Policy%20Governing,the%20Federal%20Information%20Security%20Management%20Act%20\(FISMA\)%20of](https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.361.5714&rep=rep1&type=pdf#:~:text=policy%20supersedes%20CNSS%20Policy%2019,%20%E2%80%9CNational%20Policy%20Governing,the%20Federal%20Information%20Security%20Management%20Act%20(FISMA)%20of).

Crane, Keith, Olga Olikier, and Brian Nichiporuk. *Trends in Russia's Armed Forces - An Overview of Budgets and Capabilities*. Santa Monica, C.A.: RAND Corporation, 2019.

Department of the Navy. *Littoral Operations in a Contested Environment*, Washington, DC: Headquarters, United States Marine Corps, 2017.

Department of the Navy. *The Marine Corps Operating Concept - how an Expeditionary Force Operates in the 21st Century*. Washington, DC: Headquarters, United States Marine Corps, 2016.

Department of the Navy. *MCDP 1 - Warfighting*. Washington, DC: Headquarters, United States Marine Corps, 1997.

Department of the Navy. *Tentative Manual for Expeditionary Advanced Base Operations*. Washington, DC: Headquarters of the United States Marine Corps, 2021.

Department of the Navy and United States Coast Guard. *A Cooperative Strategy for 21st Century Seapower*, 2015.

Flanagan, William D. *Flexibility in Decisive Action and Recommendations to Mitigate Risk: Electromagnetic Spectrum Footprint and Emissions Control*, CEMA, AWG, PEO C3T, CACI, 2020.

Fritz, D. A., David A. Fritz, Bharat T. Doshi, Andrew C. Oak, Steven D. Jones, Jack L. Burbank, Harry L. Miller, et al. "Military Satellite Communications: Space-Based Communications for the Global Information Grid." *Johns Hopkins Apl Technical Digest* 27, no. 1 (2006).

Harris Corporation, RF Communications Division. *AN/PRC-117G Multiband Manpack Radio Reference Guide*. Rochester, NY: Harris Corporation, 2010.

Harris Corporation, RF Communications Division. *AN/PRC-150(C) Advanced Tactical HF Radio Operation Manual*. Rochester, NY: Harris Corporation, 2007.

Jodalen, Vivianne and Terje Mikal Mjelde. *HF-Kommunikasjon i Arktis - Analyse Basert På Målinger*. Kjeller, Norway: Norwegian Defence Research Establishment (FFI), 2016.

Joint Chiefs of Staff. *Joint Concept for Entry Operations*. Washington, DC: 2014.

Joint Chiefs of Staff. *Joint Electromagnetic Spectrum Operations JP 3-85*. Washington, DC: 2020.

Kjellén, Jonas. *Russian Electronic Warfare - The Role of Electronic Warfare in the Russian Armed Forces* Swedish Defence Research Agency, 2018.

National Security Agency Central Security Service. "Commercial Solutions for Classified Program (CSfC)." Accessed February 20, 2021.

<https://www.nsa.gov/Resources/Commercial-Solutions-for-Classified-Program/Trusted-Integrators/archived/>.

Naval Network Warfare Command. *Naval Telecommunications Procedures - NTP 4 (E)* Norfolk, V.A.: Naval Network Warfare Command, 2008.

Porche, Isaac III R., Christopher Paul, Chad C. Serena, Colin P. Clarke, Erin-Elizabeth Johnson, and Drew Herrick. *Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below*. Santa Monica, C.A.: RAND Corporation, 2017.

<http://www.dtic.mil/docs/citations/AD1031235>.

The White House. *National Security Strategy of the United States of America* . Washington, DC: The White House, 2017.

The White House. *Renewing America's Advantages - Interim National Security Strategic Guidance*. Washington, DC: The White House, 2021.