Spectrum Contested Environments

Maneuver warfare and command and control in an EMS environment

by LtCol Christopher S. Tsirlis

>LtCol Tsirlis is currently the Commanding Officer of Marine Wing Communication Squadron-28.

The *Commandant's Planning Guidance* (CPG),published in July 2019*,* is the vision and strategy document that describes the Marine Corps' current and future force operational strategy to fight and win in the next five to fifteen years. Within the context of current operational realities and potential future force challenges, the document provides a foundational view for decision makers to follow and understand the direction the Marine Corps is driving toward over the next decade. The CPG recognizes the need to conduct command and control (C2) over contested networks, which can support maneuver forces in a distributed manner. The CPG also recognizes the growing threat of cyber warfare, and the Marine Corps' reliance on the electromagnetic spectrum (EMS) to conduct operations across the MAGTF must be resilient.[1] It further points out how operating in an environment where networks will be attacked, compromised, degraded, or denied is an operational reality.

Much of the focus of cyberspace operations in recent years has centered on the strategic and operational levels of war. Cyberspace is defined by Joint Publication 3-12 as a global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[2] Cyberspace constitutes three layers: physical network, logical network, and cyber-persona. The physical network component is comprised of the hardware, systems software, and infrastructure (wired, wireless, cabled links, radio links, satellite, and optical) that supports the network and the physical connectors (wires, cables, EMS frequency, routers, switches, servers, and computers).[3] The logical network layer consists of those elements of the network that are related to one another in a way that is abstracted from the physical network. An example of the logical layer is the DOD's nonsecure Internet Protocol router network. The cyber-persona layer consists of the people who are actually on the network. A single cyber-persona can have multiple users or many virtual locations, but normally not linked to a single physical location.[4] In order for networked MAGTF operations to be successful, all three layers of cyberspace operations must work effectively. The operational entities within the Marine Corps that deal with addressing cyberspace operations are the MAGTF Communications Control Center (MCCC)* and the cyberspace and electronic warfare coordination center. Traditionally the Cyberspace and Electronic Warfare Coordination Center supports MAGTF commanders use of EMS via integrated planning across the MAGTF's operational environment to increase the operational tempo and achieve military advantages.[5] Currently, this role now falls inside the MEF Information Group.

*MAGTF can denote any operational level within the MAGTF or major subordinate element. For example, a MCCC could reside at the MEF/MEB/MEU levels or at the division, air, or logistical component.

Battlefields have traditionally comprised of four domains: land, sea, air, and space. The last few decades changed the warfighting landscape to include a fifth domain: cyberspace. Some believe EMS deserves its own domain, especially considering the impacts it has on the conduct of war. Spectrum is the invisible medium that saturates the area of operations upon which the use of Marine Corps' electronic systems depend. Spectrum is a unique environment because it transcends all three levels of war and can shape tactical, operational, and strategic means and end-states on the modern battlefield. Whether the Marine Corps is operating unilaterally or as part of a joint coalition, spectrum has both enabling and restricting characteristics. Therefore, defending, controlling, and shaping the spectrum landscape can be decisive because if a unit can be seen or located electronically, it then can be attacked and destroyed.

Until very recent, the elements of the MAGTF, EMS frequency complexities surrounding cyberspace operations is given scant attention. There are many questions to consider as to the real practical impacts for maneuver forces within an EMS denied or degraded environment. Does the GCE possess the necessary capabilities to properly mitigate a spectrum contested or denied battlespace? What are the practical steps to mitigate the loss of critical C2 at the infantry battalion level or lower? Does the Marine Corps' current maneuver warfare doctrine properly support the loss of network-centric C2? Are there specific training scenarios that would help mitigate the loss of networked C2? What technologies should the Marine Corps adopt or develop to support or reinforce maneuver forces at the tactical level? What are the likely scenarios near-peer adversaries attack to limit, deny, or degrade MAGTF C2? What investments in training and technology should the Marine Corps make in order to ensure C2 of its forces during likely cyber network attacks and spectrum denied battlespaces?

While the Marine Corps has taken steps to ensure freedom of action in EMS contested environments, it has not done nearly enough to mitigate challenges of a congested radio frequency (RF) spectrum environment and the likely threats first world adversaries will impose on the battlefield to the GCE and, specifically, front line units like an infantry battalion. If tactical units cannot tie into the overall operational design of a campaign, then achieving the strategic end-state is unlikely to occur. Therefore, this article contends the Marine Corps must reexamine its current technological based C2 capabilities that enable maneuver warfare through the lens of spectrum denied or degraded operating environments. Decision makers should consider integrating readily available dynamic spectrum allocating systems and RF mapping technologies, which would significantly address key vulnerabilities that negatively affect networked C2. If adopted, they may provide the mitigation steps required to maintain decentralized C2. By waiting or failing to take steps now, the Marine Corps risks the ability to conduct decentralize decisive maneuver warfare through the use of automated C2 systems.

Methodology of Study

With the above in mind, this article explores the Marine Corps' maneuver warfare doctrine within the context of an EMS denied or the degraded environment. The current C2 structure is an operating mental framework that uses mission C2 and offers the flexibility to deal with changing situations and to exploit fleeting windows of opportunity.[6] First, the context is set by briefly examining Marine Corps maneuver warfare doctrine and key changes to C2 over the past fifteen years. Second, the framework examines the radio frequency spectrum challenges and the current communications capabilities at a typical Marine Corps infantry battalion to operate in spectrum congested environments. This article further examines some near-peer adversaries' capabilities and likely threats posed by them. In order to properly scope the topic, the article purposely does not discuss the impacts of all EMS dependent technologies such as global positioning or reconnaissance satellites, both of which would have strategic impacts for U.S. military forces worldwide. However, it is recognized that a loss of either would have significant negative impacts on Marine forces both operationally and tactically. Finally, this article will examine some emerging technologies developed by the Defense Applied Research Agency (DARPA), which, if adopted by the Marine Corps, could positively affect its ability to operate in a spectrum contested environment. Though this article centers on front line tactical units, its concepts could further be applied to both air and sea domains, regardless of echelon or scale.

Maneuver Warfare Doctrine

The Marine Corps' warfighting doctrine centers on the concept of maneuver warfare and denotes the idea of gaining a positional advantage over an adversary. While not exclusive to geographical boundaries, "this positional advantage may be psychological, technological, or temporal as well as spatial."[7] Maneuver warfare supports the philosophy of command, which requires subordinate commanders to make decisions based on higher command's intent. A commander must develop his own understanding of this intent and utilize his own initiative in order to exploit opportunities as they present themselves.[8] This concept ideally, when executed properly, generates a faster-operating tempo, which disrupts an adversary's ability to effectively resist friendly actions. Maneuver warfare, at its core, is people centric and thus does not fundamentally require external systems in order to operate. However, it requires competent leadership and high degrees of trust at all levels of the organization to be effective when employed in a decentralized manner. In modern warfare, decentralized C2 requires communications equipment.

Operating at a faster tempo requires C2 systems and structures that provide for the speed of execution of key warfighting functions. In recent years, the Marine Corps, along with the entire DOD, has sought to reduce uncertainty by dramatically increasing the amount of information utilized through networking in order to make faster decisions. This insatiable appetite for copious amounts of information has pushed the Marine Corps to move from a "people-centric" model of C2 to an information or network-centric model of C2.[9] This is evidenced by the enormous and overreliance on information systems technologies in order to operate in almost any capacity. For some, this overreliance has been seen as somewhat of an "Achilles heel" for the Marine Corps and the U.S. military as a whole. Nevertheless, the ultimate goal is to have effective C2 to mitigate the "fog of war," friction, and uncertainty of enemy actions. Effective C2 is not simply a matter of generating enough information to make a decision but rather generating the information faster with more accuracy. Ironically, this dramatic increase of information flow now means commanders run the risk of information overload with more information than can be possibly assimilated. Therefore, information for effective C2 is valuable only insofar as it contributes to effective decisions and actions. The critical thing is not the amount of information but key elements of information that are available when needed and in a useful form that improves the commander's awareness of the situation and ability to act.[10] In this way, the use of automated C2 has helped commanders enhance what is considered essential information for decision making while at the same time made it more complex and often burdensome to acquire and share it.

Marine Corps maneuver warfare doctrine does provide for effective C2 with or without information systems. However, the solution relies on training commanders and subordinates to be very comfortable in fluid and chaotic environments. A high level of trust must exist between all elements of the MAGTF. It is likely that current and future operations will require the aggregation and disaggregation of forces over a distributed area of operations to conduct expeditionary advance based operations. The reality is any distributed operations require communications systems to extend the span of control of forces. Contested EMS environments limit the friendly span of control, and maneuver warfare requires thinking of the network as a maneuver element. This enables the performance of critical C2 functions throughout operations and prioritizes support to required C2 capabilities. That is, commanders must plan for and have the capability to maneuver and adjust the network to provide C2 at decisive points and times, much like shifting and concentrating fires to impart the desired effects on an adversary. C2 structures must allow for this flexibility, and commanders and staffs must train for this eventuality.[11] Maneuver warfare theory is therefore uniquely suited for EMS contested environments because it fundamentally relies on implicit communication and mutual understanding to operate. Commanders must continue to hold to mission-type orders even while supported by networked control systems. As long as the Marine Corps continues to train with the realities of friction and uncertainty, then it is likely effective C2 will remain.

Changes in C2 over the Past Fifteen Years

Prior to the wars in Iraq and Afghanistan, the Marine Corps generally followed the people centric C2 model and was comfortable relying on single channel radio, implicit communications, and commander's intent to make faster decisions than its adversaries. However, the Marine Corps also recognized the necessity to use key technologies, which supported decentralized C2. As a result, since 2003 and because of the wars in Iraq and Afghanistan, the Marine Corps has expanded almost every method of communications technology available today. For example, in 2002, the average Marine Corps infantry rifle company only processed five Very High Frequency (VHF) tactical radios to facilitate C2. Today, almost every Marine possesses some type of communications device to support C2. Larger maneuver units have also increased the use of high bandwidth terrestrial and satellite systems for C2. This accounts for almost a 200 percent increase in communications technologies within the GCE. Therefore, without any formal change to its warfighting doctrine, the Marine Corps has shifted from a people-centric to information system-centric C2. On the surface, this is not a negative factor and, arguably, the rapid proliferation of communications technologies has directly facilitated the concept of maneuver warfare because these technologies have increased the operating tempo of all Marine Corps warfighting functions. Conversely, this dramatic increase in communications equipment has amplified the need for more expeditionary power sources to operate the demand. Large battalion command posts and company footprints require more tactical power sources that leverage a networked C2 posture. Additional power sources require more logistic trains, such as fuel, and create additional vulnerabilities that can negate the advantages of the Marine Corps' maneuver warfare doctrine. A case can be made the average Marine Corps infantry battalion is actually slower and more vulnerable today based on its overreliance on communications systems and the logistics tail required to support them. In addition, there is a generation of Marines who have grown accustomed to operating in large logistical footprints.

In practical terms, the average infantry battalion in the Marine Corps is the base unit for combat operations within the construct of the MAGTF. This design requires the Marine Corps operating in an integrated task force fashion, which will be ready to address any crises as they arise through the use of power projection from the sea and the use of expeditionary locations. The infantry battalion, with the use of its organic communications enablers, are designed to utilize maneuver warfare and conduct C2 in multiple ways. The use of line-of-sight (LOS) systems is the primary means for data and voice communications. In recent years, the use of beyond-line-of-sight (BLOS) C2 systems has grown to meet the need for distributed operations. LOS systems are most closely related to tactical radio systems. BLOS systems are usually associated with satellite or tropospheric technologies. GPS are also included in BLOS systems but are mostly associated with the position, navigational information which facilitates friendly and enemy locations, fires, and other automation. For the purposes of this article, GPS is excluded from analysis but should be considered linked to other satellite technologies in terms of capabilities and vulnerabilities.

> ***In practical terms, the average infantry battalion in the Marine Corps is the base unit for combat operations within the construct of the MAGTF.***

The Radio Frequency Spectrum

One of the biggest challenges for military communications is dealing with the RF spectrum. The RF spectrum is a commodity that is infinite supply and heavily regulated, both in and outside the United States.[12] Military communications equipment, civilian communications infrastructure, and countless other technologies, specifically anything with an RF emitter, must compete for available spectrum in order to operate. Entire government and commercial enterprises are centered around proper

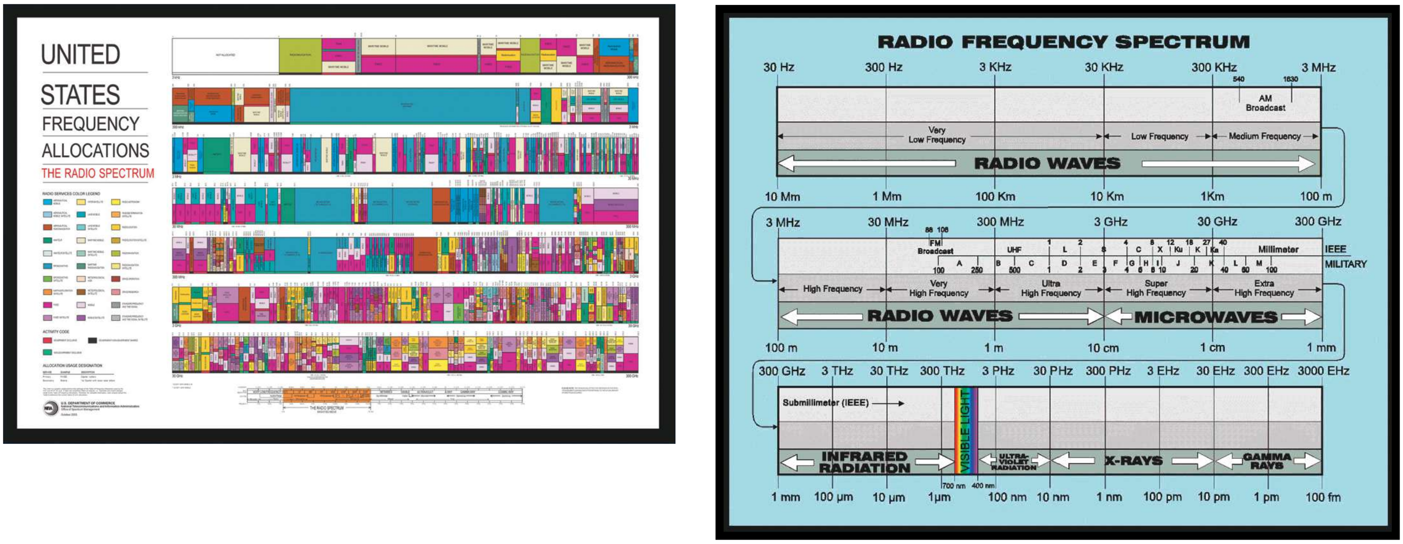

Figure 1. APPENDIX A: Frequency Spectrum Charts. The United States Frequency Allocation Chart. Source: U.S. Dept. of Commerce, National Telecommunications and Information Administration, Office of Spectrum Management, March 1996.

spectrum allocations. Communications technologies rely on the enforcement and regulation of spectrum access (Appendix 1, Figure 1 illustrates the congested spectrum in the United States alone). For the DOD there are specific RF spectrum areas that allocate for military use only (Appendix 1, Figure 2). Unfortunately, certain areas of the spectrum permitted inside the United States are not allowed in other countries. The U.S. military lacks authority to transmit on all desired frequencies while outside of the continental United States (OCONUS) because of interference with other host-nations' communications infrastructures. Therefore, host-nation approval is required before utilizing those frequencies. Despite the escalating demands on available spectrum, only about five percent is used at any given time, which is an incredibly inefficient use of space.

Military communications at the infantry battalion level fall at all ends of the RF spectrum range. Most tactical radio communications use a variety of high frequency (HF), VHF, and ultrahigh frequency (UHF). Almost all wideband satellite communications use super high frequency and extremely high frequency.[13] Communication channels are often broken down further into narrowband and wideband channels in order to denote the amount of bandwidth available to operate. Narrowband technologies, under 25 kilohertz (KHz), usually support voice, positional, and limited data communications.

Narrowband technologies are used heavily to support maneuver and fires because of their reliability and mobility over uneven terrain. Wideband technologies are usually anything channeled over narrowband but also utilize all elements of the spectrum to support large amounts of data and voice communications. Most often they operated in megahertz (MHz) channel spaces and can often provide much larger bandwidth capabilities to support network-centric operations. Wideband technologies require significantly more power and are usually static in nature. However, in recent years, mobile wideband technologies have begun to emerge and show great promise for future MAGTF operations. As a rule, all military communications employ communication security protocols and encrypt both data and voice signals to ensure the integrity of information delivered. In addition, many narrowband systems utilize frequency hopping algorithms and sophisticated waveforms to thwart any adversaries' attempts to frequency jam friendly communications signals. Finally, the manipulation of the RF spectrum has enabled C2 in many positive ways. The key is finding ways to optimize it once it becomes contested.

Spectrum in a Contested Battlespace

Since 2003, and as a counterbalance to the growing threat of insurgent attacks via IEDs, the Marine Corps began to adopt a host of jamming technologies in order to counter or defeat the threat posed by IEDs that are command-detonated by radio signals. During the early stages of the Iraqi campaign, Marine communicators at the infantry battalion level had to develop best practices for operating in highly congested spectrum environments like Ramadi and Baghdad.[14] Eventually, the Marine Corps successfully integrated these systems into their C2 infrastructures, often through trial and error and planned design. Additionally, successful techniques, tactics, and procedures only developed once the campaign slowed to counterinsurgency operations operating from fixed forward operating bases. There were not spectrum sensing technologies available to ensure enemy forces were not denying or disrupting operations. Even today, there are no RF sensing tools organic to an infantry battalion's communication platoon. Ideally, a reconnoiter of the spectrum environment would help Marine communicators understand if there is probable or current interference with their communications systems. As such, it is often through the arduous task of trial and error, loss of vital communications links, and placement of

Russian Jamming Equipment/Spectrum Range	Spectrum/Frequency Range	Jamming Range/Bandwidth/ Power	# of Radio links suppressed quasi-simultaneously	U.S. Radio Equipment Affected	Effects on USMC C2
R-325U[34]	HF/1.5-29.9999 MHz	60Km	4	PRC-150/VRC-148	Degrade/Denial
R-378A[35]	HF/1.5-30 MHz	target 3.0, 10.0, 20.0, 50.0 kHz; barrage 150-8,000 kHz	up to 3 FF; programmed FH 1	PRC-150/VRC-148	Degrade/Denial
R-934B[36] automated station is designed for jamming FF and FH ground fixed and mobile communication systems, and cellular and trunk networks	VHF/UHF/100-399.995 MHz	Programmable/ Output Power Dependent	4	PRC-117GMP PRC-152HH PRC-148HH	Degrade/Denial
R-330T[37] automated jamming station is designed to jam VHF tactical communication links operating in FF and adaptive and programmed FH modes.	VHF/30-99.999 MHz	Programmable/ Output Power Dependent	FF up to 3; programmed FH 1	PRC-117F/G, MRC-145	Degrade/Denial
RP-377VM1 RP-377UVM2, and RP-377UVM3 (small port size)[38]	20-1,000 MHz	Designed for the jamming and blocking of radio communications and control, both when stationary and on the move	Broadband noise barrage jamming is provided both over the whole operating frequency range and in any combination of the transmitters' frequency sub-bands. Can be mounted on wheeled and tracked vehicles	All current USMC, VHF, UHF tactical radio systems	Degrade/Denial
SEL SP-162[39] 'Batog' cellular jammer	(Band no 1, CDMA-450 standard) 463 - 467 MHz (Band no 2, GSM-900 standard) 935 - 960 MHz (Band no 3, GSM-1800 standard) 1805 - 1880 MHz (Band no 4, UMTS (3G) standard) 2100 - 2170 MHz	Based on advanced cellular jamming technology, the 'Batog' transmits an RF signal which blocks the communication between a mobile phone and a cellular base station Explosive Devices (IEDs).	On the customer's request the jammer can be manufactured with four bands of any other cellular standards.	Cellular Phones – All types	Degrade/Denial
AURA[40]	GPS (L1, L2, L5), CDMA, GSM-900, GSM-1800, DECT, 3G-1, 3G-2, 3G-3, WiFi	60-500m		Cellular Phones – All types	Degrade/Denial

Figure 2. APPENDIX B: Russian Land Based Jamming Equipment. (Not all inclusive). Location of Most Military RF Spectrum. Source: Borner, Katy, Atlas of Science: Visualizing What We Know, (2010). The MIT Press, *page 112.)*

key retransmission nodes that a robust communications architecture can take form. The inability to conduct RF sensing operations does present a real and likely vulnerability for an adversary to exploit. The incapacity to quickly identify the source of interference and take mitigation steps could prove disastrous for maneuver forces.

Current and Likely Threats Posed by MAGTF Adversaries

Arguably, Russian and Chinese military forces pose the greatest near-peer technological threat to the Marine Corps' ability to C2 its forces. Both countries have existing spectrum disrupting capabilities which could deny or significantly degrade Marine Corps tactical C2 systems. The negative impacts are many. A cursory examination of recent Russian and Chinese military activities can provide a sense of how each country could seek to counter the Marine Corps ability to C2 maneuver forces, conduct integrated fires, and maintain information superiority on the battlefield.

Russia. Russian military forces possess an array of jamming capabilities which operate across all areas of the spectrum. In every area where the Marine Corps operates its critical radio frequencies is where electronic countermeasures could be employed. An example of Russian military cyber warfare tactics manifested with its war with Georgia in August 2008 and most recently with its conflict with Ukraine. In both cases, Russian conventional military attack was complemented by a series of cyber-attacks targeting key networks of Georgian institutions, the media, and even the country's government. When Russian tanks crossed the border into Georgia, network denial of service operations was conducted against the computer systems of Georgia. The targets of the cyber-attack were Georgian government websites and even included websites of the United States and British Embassies. The attacks initially came from Russian IP addresses, which resulted in a cyber blockade that perfectly correlated with the Russian military actions to make its offensive more successful. For these reasons, this type of cyber-attack should be considered an operational approach likely used by the Russian military that prepared the battle-space for a Russian military invasion of Georgia.[15] The effects of the cyber operation had little to offer in the terms of severity. No one killed as a direct result of the operation and no property damage occurred, but it

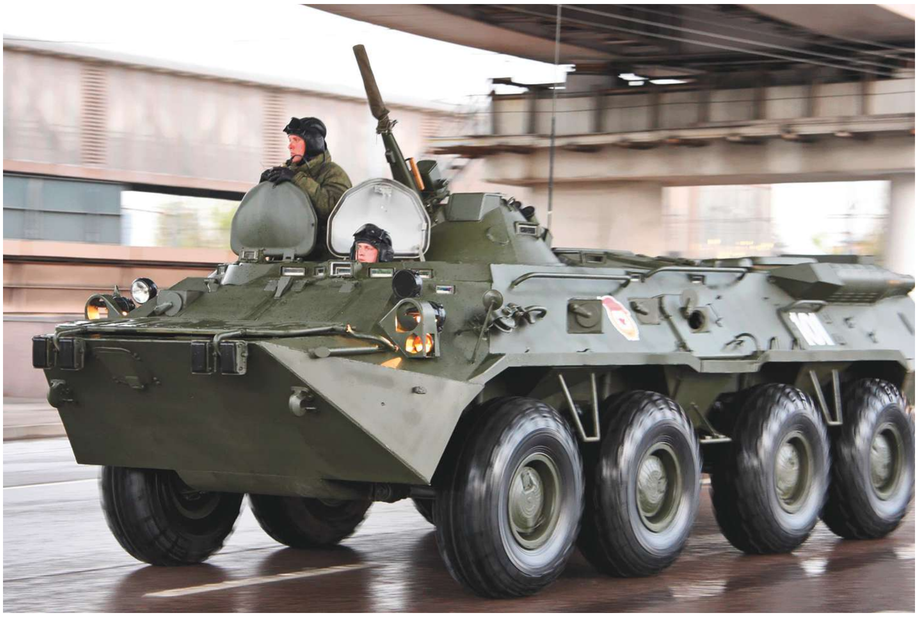

Figure 3. The Russian military has the capability to employ the BTR-80 with mounted jamming equipment. ***(Photo by Vitaly V. Kuzmin and is licensed under Creative Commons Atribution-ShareAlike 4.0 International license.)***

does offer a glimpse as to the combined armed nature cyber operations will be used in conjunction with traditional military forces.

Russia's computer network attacks against Georgia during the South Ossetia conflict are best characterized as a digital blockade of information. As recent as last March, Russians have developed systems mounted on land-based vehicles, helicopters, and ships to jam military communications and weapons from several hundred kilometers away.[16] It is likely, whether through the use spectrum interference or Internet style attacks, that the ability to 'block" Marine Corps C2 systems is a tactic to be employed by a near-peer competitor like Russia. Therefore, strategic options and the operational design of any campaign may have to change for joint force commanders if cyber operations are likely to occur. For example, the strategic option of sea-based forcible entry operations, a core MAGTF mission, may be negatively affected if critical C2 systems are degraded or denied in an operational environment.

As recent as 2015, the Russian military has completely upgraded its suite of land-based jamming equipment capable of detecting and suppressing mobile satellite communications and navigation signals, as well as jamming tactical communications networks in the HF through the UHF range. Tactical impacts are clear, but operational and strategic maneuver are affected as well. By employing four different software-controlled jammers, it is replacing the earlier systems to cover the full RF spectrum. For example, the most recent Russian electronic warfare system is a multifunction system mounted on a BTR-80 armored personnel carrier (see Figure 3). It is designed to protect land units from mines and remote-controlled improvised explosive devices, as well as jamming tactical communications.[17] Appendix B/Table 1 (on page 75) reveals Russia's full spectrum capabilities to deny or degrade Marine Corps tactical communications systems.

Russia's capabilities also extend into the counter-space capabilities sphere. As recent as December 2016, Russia conducted a successful test of an anti-satellite weapon.[18] There may be a variety of ways to degrade or destroy a satellite. Russia has demonstrated the ability to simply develop kamikaze satellites designed to disable other satellites by crashing into them.[19] Although the United States has a multitude of spacecraft that facilitate ground-based C2, the impact of disabling key wideband satellites over a particular geographic area would have negative impacts on Marine forces.

If the Marine Corps ever faced Russian conventional forces, it is very likely the ability to C2 would be severely compromised or denied. Even a non-kinetic confrontation could lead to a severe enough degradation of networked C2, which would inevitably limit the span of control and dramatically shorten lines of communications of ground forces. GCEs such as infantry battalions possess no organic ability to scan the RF spectrum in order to understand the impacts on their critical communications links. Since most direct combat formations conduct operations over voice and data communications links, Russian targeting whole frequency ranges and frequency hopping algorithms could lead to a virtual breakdown of C2. A breakdown of C2, therefore, eliminates the ability of the MAGTF to conduct maneuver and combined arms operations.

People's Republic of China. China is another potential near-peer adversary who has demonstrated the capacity to target one of the most widely used communication technologies by the United States: satellite technology. Over the past fifteen years, the Marine Corps has dramatically expanded its use of digital C2 networks over satellite transmission links. First in 2007, and then later in 2013, China successfully tested the use of anti-satellite weapons.[20] These tests illustrate a clear warning as to the critical vulnerability U.S. forces have against the loss of critical communications architecture. Furthermore, China is capable of developing ground-based lasers, space jamming technologies, and microsatellites to attack U.S. space assets.[21] China recognizes the asymmetric benefit that U.S. forces gain from space—through the use of reconnaissance and communications spacecraft—and is employing counterstrategies designed to deprive the United States of this lopsided advantage. For example, Chinese military writings

> "emphasize the necessity of 'destroying, damaging, and interfering with the enemy's reconnaissance … and communications satellites.[22]

Crippling or degrading these systems exploits a critical vulnerability for the United States.

The employment of anti-satellite weapons by China is problematic on two fronts. First, such action would completely change the ability of ground maneuver forces to communicate via BLOS digital or voice networks. As a result, almost all information superiority stemming from high capacity digital networks, which ride satellite transmission paths, are disrupted or denied. Second, distributed combat formations would necessarily shrink in order to keep critical lines of communications open. Mass distributions of information are then regulated to wideband terrestrial communication links and are traditionally limited to 30 miles or less. Only voice communications would remain. Couple the RF jamming threats referenced above by Russia, the average Marine Corps infantry battalion relegates C2 distances similar to World War II formation in the Pacific Theater. Given the distributed nature in which the MAGTF operates most effectively today, such a loss would dramatically weaken the combined-armed nature in which the MAGTF fights.

Emerging threats. Other potential adversaries that could employ technologies which would counter the Marine Corps C2 capabilities are actors such as Iran or North Korea. Each of these countries possesses electronic countermeasure capacities which are certainly a derivative of both Russia and China potential employment strategies. More recently, the commercial off-the-shelf software has allowed nations like Iran and North Korea to wage theoretically bloodless offensive cyber-attacks against well-established powers. For example, in December 2009, an unsecured downlink from a U.S. military unmanned aerial vehicle (UAV) was intercepted by Iran using a $25 piece of file-sharing software, called "skygrabber," originally developed to intercept satellite television feeds.[23] Additionally, in December 2011, Iran claimed it hacked the GPS signal of a U.S. Lockheed Martin RQ-170 Sentinel UAV (see Figure 4).[24] Iran landed it near Kashmar—about 225 km inside northeastern Iran. Twelve months later, Iranian television then broadcast footage of a Boeing Scan Eagle long-endurance UAV (see Figure 5), which they claimed had been hacked by Iran.[25] Iran and North Korea are known buyers of sophisticated weaponry and are no less capable in their ability to disrupt C2. It is clear both countries view the EMS as an area to conduct combat operations.

Figure 4. Lockheed Martin RQ-170 Sentinel UAV. ***(Drawing by FOX52 and is licensed under Creative Commons Atribution-ShareAlike 4.0 International license.)***

Radio electronic combat (REC) is the integration of signals intelligence, target acquisition, and electronic attack/protection. The Democratic People's Republic of Korea , [North] Korea People's Army , the People's Republic of China (PRC), Chinese People's Liberations Army (PLA), and the ground forces of the Russian Federation all employ variations of REC. The core of enemy REC lies in the sequence of activities that attempt to selectively deprive MAGTF forces of tactical electronic support assets. REC priorities depend on the tactical situation and level of command but could include targeting fires and air forces. Command posts, key logistic sites, and point targets that menace enemy forces may also be possible targets. Likely tactics, techniques, and procedures may or may not include disrupting C2 links below the battalion level; however, given the trend of MAGTF operations in a dispersed manner, any disruption could be lethal for friendly forces. Simple direction finding can precisely provide the location of friendly forces, which can easily provide targeting information for adversaries. Any concentration of radio signals can paint a picture for enemy forces to exploit. The use of high-energy radio frequency guns can reach hundreds of meters or more through pulsed or continuous sine waves which can degrade or damage communication systems from high voltage spikes.[26] The success of REC depends on many factors but does not need to be decisive to be completely effective. Merely limiting the effects of friendly intelligence gathering tools limits the ability of MAGTF forces to conduct detailed planning. Massing jamming of friendly narrowband radio circuits during amphibious operations or other maneuver operations strikes at the center of friendly concept of operations.

In terms of relative combat power, the United States is certainly dominating in many areas. However, adversaries such as Iran and North Korea only need to conduct a simple calculation of where to apply pressure in order to mitigate any U.S. technological advantages. By attacking or disrupting friendly C2, the speed and lethality of the Marine Corps maneuver forces are quickly di-

Figure 5. Boeing Scan Eagle long- endurance UAV. ***(U.S. Navy photo.)***

minished—if attacked properly. The question is not whether near-peer adversaries or other state actors possess the ability to affect Marine Corps C2, but rather, what steps can the Marine Corps take to mitigate against it. Although technology is not the only answer, it does provide avenues to pursue and consider.

Technological Mitigation Techniques

Historically, uncertainty is considered a fundamental aspect of warfare. Despite this, the pursuit of certainty for more effective C2 information systems remains. The DARPA has recognized this problem for DOD and has some unique solutions to address spectrum denied/degraded environments. The challenge for DOD is not the ability to develop new anti-jam tactical radio systems but rather to make a business use-case for the defense industry to develop such technologies on their own accord. It is feasible to produce tactical radios at $1,000-1,500 per unit vice the $20-25K per average unit cost now. This is largely because of the adoption of low-cost field-programmable gate arrays and integrated circuits (ICs) which can implement complex digital computations and interconnects embedded microprocessors on current tactical radios systems. DARPA believes this industry trend of using field-programmable gate arrays and ICs will only increase the power and capabilities of radio systems.[27] As the costs go down, so does the size. The radio circuit industry has continued to outpace the speed of delivery to Marine Corps tactical units. Newer ICs combine entire RF, analog, and digital front ends of radios with high-bandwidth heterogeneous multiprocessor-based computations all on one integrated circuit. The radio manufacture industry is capable of providing what the MOC infers needed for all Marine forces: C2 via voice/data that is ubiquitous with the equipment attributes of low size, weight, and power consumption.

Dynamic Spectrum Access

DARPA, through its next generation program, has developed technologies which utilize the EMS more effectively and thus may help the Marine Corps mitigate against those near-peer threats outlined previously. These technologies come in the form of a cognitive radio technology, which dynamically uses available RF spectrum in a unique way. DARPA refers to the technology as dynamic spectrum access (DSA) radio technology. DSA is a cognitive radio system that has the ability to detect and recognize its settings—in order for it to adjust its radio operating setting dynamically and autonomously—and to learn from the results of its actions and its operating framework. A cognitive radio is a form of wireless communication in which a transmitter or receiver can logically detect which communication channels are in use and which are not and can transfer communications to the unused channels. This allows optimum use of the available radio frequencies within a given spectrum space while minimizing interference with other users. It can adjust the operating settings of the radio's frequency in a network node. For example, the range of frequency, the type of modulation, and the power output all occur dynamically.[28] Because of the enormous algorithmic computations that must occur, cognitive radios are software defined radios. A software defined radio is an enabling technology for cognitive radios because of the flexibility, reconfigurability, and portability inherent to the cognitive radio's aspect of adaptation.[29]

The unique attributes of such a technology provide for a host of opportunities for the Marine Corps communications community. Specifically, for infantry battalions, this technology allows for mobile and static radios networks to adapt to unfavorable spectrum conditions, therefore offering network users simpler, effective, and complete access to clear frequencies. Cognitive radios using DSA technology also offer a solution to the problem of spectrum crowding (degraded communications) or jamming (denied communications) by giving priority to a spectrum owner, then allowing others to access it by using available parts of the spectrum. When unauthorized users are detected on the same channel, a DSA-enabled device instantly moves to vacant channels. Since many RF frequencies use only a small portion of the time and in a fraction of locations, DSA technology enables more networks to share a given spectrum band. This is particularly useful for dense urban terrain or in megacity environments. Since it is likely that future conflicts will occur in highly populated and littoral areas where spectrum availability are further complicated by host-nation internal rules or unfriendly neighboring states emissions, DSA technology provides the least intrusive method of spectrum dominance. Freedom of action in the electromagnetic battlespace will be the responsibility of spectrum managers who must carefully balance the requirements of Marine forces and the capabilities of each equipment set used for combat operations.

Marine Corps spectrum managers currently apportion CONUS and OCONUS frequencies based on national policy and regulations, unit priority, geographic location, system capabilities, and host-nation agreements. To assist in this management, DARPA also has shown that DSA-enabled radios can be programmed with policy modules so that no matter where in the world the radio is located, they can automatically adhere to spectrum usage policies. This is particularly useful for MAGTF G-6 planners because they can institute policies that more precisely enable or restrict communications within the particular geographic area. Ideally, cognitive systems would allow Marine communicators to enter into an environment not knowing anything about adversarial systems, understanding them, and even devising operational countermeasures rapidly.

Dynamic spectrum access technology mitigates an enemy's ability to dynamically jam a whole range of friendly frequencies at the exact same time with variable levels of power because the cognitive nature of the technology will dynamically switch to areas of the frequency spectrum which are unmolested. Cognition in this space is essentially applying machine learning to make systems smarter than the enemy can react. If the enemy switches its radio countermeasures approach, the technology will dynamically move, based on preconfigured policies, without user knowledge and thus maintain vital communications services. Radio network operators can provision a range of spectrum management policies such as interference levels, transmit power, consumption limits, co-existence thresholds, and allocation methodologies. Such capabilities allow for realtime spectrum deconfliction with friendly counter radio electronic warfare systems and congested noise floors in urban environments.

Mapping the RF Environment

Adopting a new technology like DSA only provides a limited mitigation for spectrum denied or degraded environments. Although it uses the spectrum more efficiently for communications, it does not provide enough spectral situational awareness for the average Marine Corps infantry battalion. The vital question remains: how does an infantry battalion know what is affecting its radio network if it does not possess the capability to sense the spectrum in a meaningful way? Outside of the electron warfare or signals intelligence community, which reside outside the infantry battalion, there is no realtime ability for infantry battalions to understand its frequency battlespace. To date, the focus of effort for spectrum sensing technologies in DOD has been to facilitate targeting, electronic warfare, and intelligence collections activities. However, because of the limitations of doctrinal employment and security protocols, the trilateral synergy between those communities and the general communications systems community are very weak.

There are great advantages for spectral sensing for C2 systems planning and shaping. Understanding and planning electromagnetic spectrum operations based on seeing and sensing the spectrum environment can be a vital capability for infantry battalions. Currently, the infantry battalion S-6 sections operate blind, in a spectrum sense, when planning and executing communication plans. If and when RF inference occurs, there is no current way for Marine infantry battalions to determine whether it is occurring from urban noise, other transmitting systems, or jamming by adversarial entities. There is no current method in place which is organic to conduct a reconnaissance of the spectrum battlespace in order to ensure frequency assignments are optimal to support the communications plan.

Radio Map

DARPA has developed a technology called RadioMap that increases planning, de-conflicting, validating, or shaping spectrum support to the electronic warfare, signals intelligence, and C2 communities. At a minimum, there is a prospect to expand the scope of this capability to exchange realtime electromagnetic environment data with other C2 RF propagation tools and an opportunity to work on the collaboration piece of electromagnetic spectrum operations between operations, intel, and the communications communities within the Marine Corps.

The DARPA solution is quite unique and leverages existing RF sensing architectures and uses to act as distributed sensors on the battlefield. The approach centers on efficiently managing the congested RF spectrum by providing realtime awareness of radio spectrum use across frequency, geography, and time. The output of the technology is a map that gives an accurate picture of spectrum use in in any environment. This enabling technology can generate tempo and speed by identifying problems caused by spectrum congestion and potential interference problems. The program uses existing tactical radios and jamming devices deployed for other mission purposes and uses the capabilities of these modern radios to sense the spectrum when they are not communicating. Using distributed high-density sensors can generate very sophisticated views of what is going on in a complex and RF congested environment.[30] RadioMap enables operators to see where RF conflicts exist, or even anticipate where they might occur, and find unused frequencies to utilize in order to improve the effectiveness of tactical missions.[31]

The creation of a realtime map can be likened to traffic cameras in urban areas that present the flow of traffic congestion during different periods of the day, providing awareness of a road. RadioMap is designed to help see and avoid congestion. Unlike DSA, RadioMap is not designed to deal with external transmission systems but rather to identify frequency usages and to help determine if preplanned or existing radio frequencies are clear or jammed. Hence, allowing better planning and allocation of the RF spectrum to units operating in RF congested, denied, or degraded environments. A significant derivative of RadioMap is the ability to use existing radios or jamming equipment already used by infantry battalion units and, in essence, would conduct multiple functions to inform the Marines about threats and targeting opportunities that are visible in the RF spectrum. Ideally, future mapping systems would enable Marine operators to undertake realtime reconfiguration and simultaneously conduct jamming/transmitting or surveillance/receive missions, so that infantry forces can benefit from a range of tasks from electronic intelligence gathering, electronic protection/attack, communications jamming, or electronic support measures without having to rely on external attachments from the signals intelligence battalions.

Remote control improvised explosive devices use a variety of transmission systems to enable detonation. Any electronic device with enough power to detonate a blasting cap has been used to initiate attacks.[32] Since RadioMap uses existing tactical radio networks to sense the electromagnetic environment, small tactical units such as infantry platoons could monitor radio transmissions and other RF transmitting devices in order to exploit opportunities and mitigate potential threats. The practical application of situational awareness in the RF environment can constitute a force protection measure for ground forces. From an intelligence gathering perspective, ground units outside the signals intelligence community would be able to observe transmissions and determine the type and characteristics of any RF emitting devices within a given radius.[33] The benefits of seeing the "unseen" displayed on a graphical map would shape combat operations and allow small unit leaders to exploit enemy activities by rendering devices like remote-controlled improvised explosive devices less effective. Of course, improvised explosive device mitigation is but one of multiple applications RF sensing technologies could be used for. The ability to "see" how crowded the airwaves are allowed for Marines to understand how to optimize internal networks against outside interference.

Conclusions and Recommendations

The real challenge to C2 posed by contested EMS environments is not just about technology fixes or organizational changes but rather about recognizing critical vulnerabilities and hardening these areas to mitigate the threat from adversaries. The approach explored in this article posits there are specific technologies available today which can help Marine infantry battalions navigate likely electronic cyber-attacks on their tactical C2 systems. Just as a commander would use combined arms or reconnaissance assets to control or understand their operating environment, there should be efforts to help Marine communicators adjust to the electromagnetic operating environment.

As noted before, C2 is uniquely a people-centric enterprise, but one that is made more efficient through the use of information-centric systems. EMS is a unique operating environment because it transcends all three levels of war and because can shape tactical, operational, and strategic means and end-states on the modern battlefield. C2 systems allow for speed in the decision-making process as well as disaggregated operations which underpinned the *Marine Corps Operating Concept;* however, the heavy reliance on these information systems creates a new set of critical vulnerabilities which strike at the heart of the MOC.

We are competing against near-peer adversaries who possess disruptive EMS technologies and other methods to counter our traditional military advantages. The Marine Corps must invest in technologies that ensure it can dominate any EMS contested environments. DSA and RadioMap technologies are some methods in which this can be done. Both of these technologies have the potential to significantly offset the growing capabilities of our adversaries. They also expand the operating abilities of Marine infantry battalions' communication platoons by providing cognitive adapting technologies which allow for greater battlefield awareness.

In the end, the challenge of operating in EMS contested environments is a topic which requires future research. Some recommended topics include a cost-study which examines the feasibility to rapidly upgrade or replace vulnerable information systems. Another would be the organizational changes in training and education which would be required to integrate these technologies into the GCE. If the Marine Corps waits to address this problem, then future adversaries will not and will continue to gain momentum in their efforts to thwart our military dominance. We must embrace this reality and adopt technologies that ensure the Marine Corps will succeed no matter which operating environment it fights in.

Notes

[1] Gen David H. Berger, *38th Commandant's Planning Guidance*, (Washington, DC: 2019).

[2] Joint Staff Director of Operations, (J-3), *Joint Publication 3-12 (R), Cyberspace Operations*, (Washington DC: Department of Defense, February 2013).

[3] Ibid.

[4] Ibid.

[5] Headquarters Marine Corps, *Marine Corps Interim Publication 3-40.04, MAGTF Electromagnetic Spectrum Operations*, (Washington, DC: January 2015).

[6] Headquarters Marine Corps, *MCDP 6, Command and Control*, (Washington, DC: 1996).

[7] Headquarters Marine Corps, *MCDP 1, Warfighting*, (Washington, DC: 1997).

[8] Ibid.

[9] Christopher Tsirlis, "Overreliance on SATCOM," *Marine Corps Gazette,* (Quantico, VA: September 2011).

[10] Paul Stokes, "The Will to Communicate," *Marine Corps Gazette*, (Quantico, VA: September 2016).

[11] Ibid.

[12] Christopher Tsirlis, "The RF Spectrum Battlespace," *Marine Corps Gazette,* (Quantico, VA: March 2011).

[13] Ibid.

14. Author's personal experience while serving as an Infantry Battalion S-6 for 2d Battalion, 5th Marine Regiment, Operations IRAQI FREEDOM I and II.

15. Joseph Bussing, "The Degrees of Force Exercised in the Cyber Battlespace," *Connections: The Quarterly Journal,* (Sofia,BG: Procon, Ltd., 2013).

16. Jaroslaw Adamowski, "In Shadow of Russian EW might, Baltics Take Action," *Defense News*, (October 2015), available at https://www.defensenews.com.

17. Zòrd, "New Jammers for Russian Land Forces," *Journal of Electronic Defense,* (Gainesville, FL: Association of Old Crows, 2016).

18. Weston Williams, "Russia Launches Anti-Satellite Weapon: A New Warfront in Space?," *Christian Science Monitor*, (Boston, MA: Christian Science Publishing Society, December 2016).

19. Ibid.

20. Yasmin Tadjdeh, "New Chinese Threats to U.S. Space Systems Worry Officials," *National Defense,* (July 2014), available at https://www.nationaldefensemagazine.org.

21. Jeffrey Lewis, "False Alarm on Foreign Capabilities," *Arms Control Today,* (2004), available at https://www.armscontrol.org.

22. Office of the Secretary of Defense, Annual Report to Congress: "Military and Security Developments Involving the People's Republic of China 2015," (Washington, DC: April 2015).

23. Staff, "Intelligence Intercepted," *Air Force Times*, (Springfield, VA: December 2009).

24. Jeremy Binnie, "Iran Releases Footage from Captured RQ-170," *Jane's Defence Weekly,* (London, UK: 2013).

25. Farnaz Fassihi, "Iran Claims it Captured U.S. Drone," *Wall Street Journal*, (New York, NY: December 2012).

26. Dorothy E. Denning, *Information Warfare and Security,* (New York, NY: ACM Press Books, 1999).

27. Discussion between John Flanagan, DARPA, Scientific, Engineering, and Technical Assistance (SETA)/Adaptive Execution Office (AEO), and author on 13 October 2016.

28. Benmammar Badr, and Amraoui Asma, *Radio Resource Allocation and Dynamic Spectrum Access*, (Somerset, US: Wiley-ISTE, 2013).

29. Ibid.

30. Geoff Fein, "Lockheed Martin Effort Links RF Receivers to Create an EM Spectrum Map," *Jane's International Defense Review*, (December 2016), available at https://www.janes.com.

31. Kevin McCaney, "Uncluttering the Spectrum by Putting it on the Map," *Defense Systems*, (November 2015), available at https://defensesystems.com.

32. Author's personnel experience in Iraq 2003-2005. Remote control improvised explosive devices have been denotated with a variety of transmission devices to include, cellphones (UHF), long-range cordless phones (VHF), and tactical radio equipment (HF/VHF/UHF).

33. DARPA, "DARPA's Advanced RF Mapping (RadioMap) Program-RF Café," Defense Advanced Research Projects Agency, (November 2013), available at https://www.darpa.mil.

34. IHS Jane's, "R-325U HF Automated Jamming System," (April 2016), available at https://janes-ihs-com.lomc.idm.oclc.org.

35. IHS Jane's, "R-378A HF Automated Jamming Station," (April 2016), available at https://janes-ihs-com.lomc.idm.oclc.org.

36. IHS Jane's, "R-934B VHF Automated Jamming Station," (April 2016), available at https://janes-ihs-com.lomc.idm.oclc.org.

37. IHS Jane's, "R-330T VHF Automated Jamming Station," (April 2016), available at https://janes-ihs-com.lomc.idm.oclc.org.

38. IHS Jane's, "RP-377 Series Radio Reconnaissance, DF, and Radio Countermeasure Family," (April 2016), available at https://janes-ihs-com.lomc.idm.oclc.org.

39. IHS Jane's, "SEL SP-162 'Batog' Cellular Jammer," (September 2015), available at https://janes-ihs-com.lomc.idm.oclc.org.

40. IHS Jane's, "AURA Mobile Communications GPS/WiFi Jammer," (December 2015), available at https://janes-ihs-com.lomc.idm.oclc.org.

>Note: Footnotes 34–40 are in Figure 2.