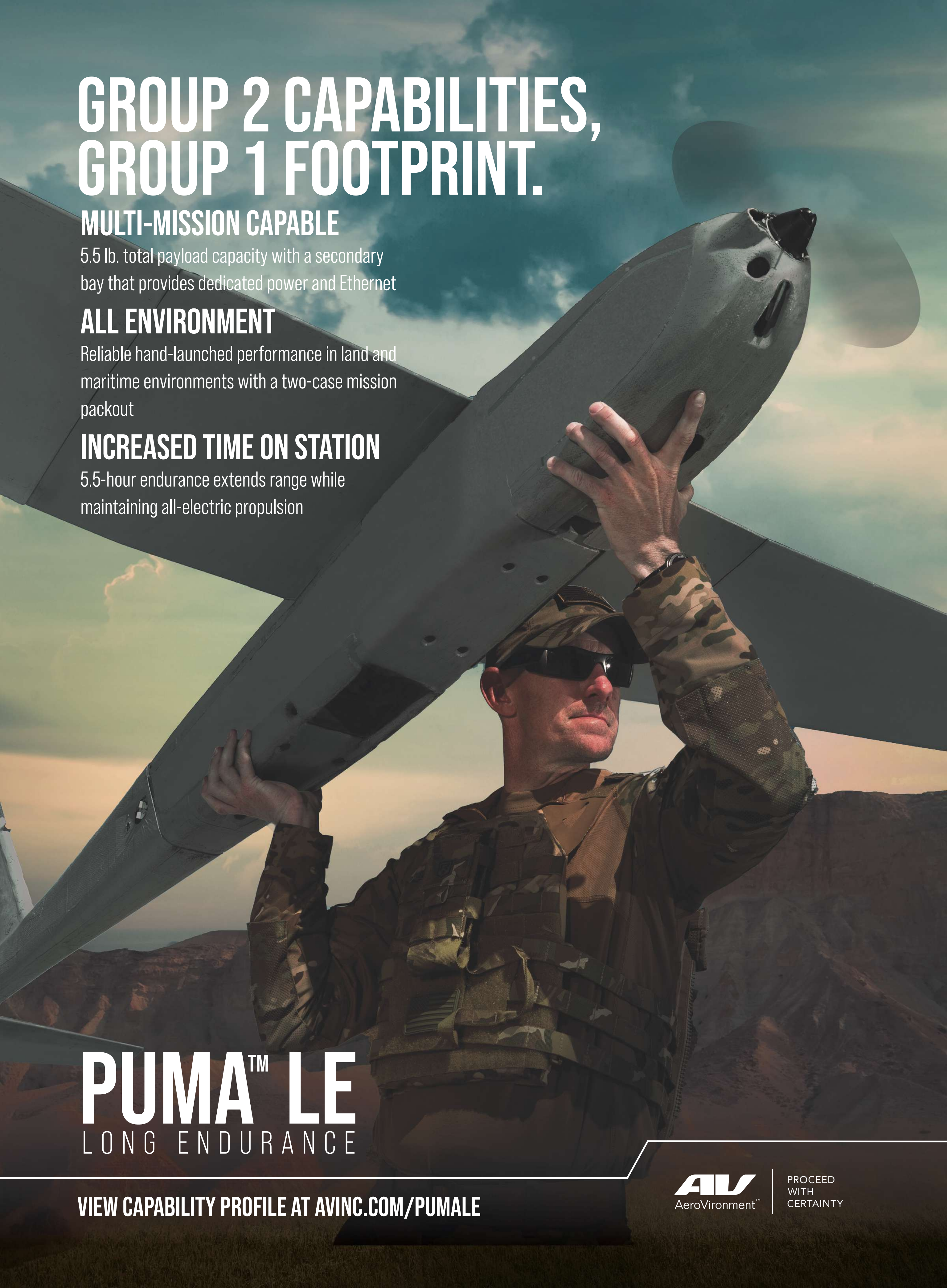
MARINE CORPS
Gazette
Professional Journal of U.S. Marines

APRIL 2020 Vol. 104 No. 4 www.mca-marines.org/gazette

A publication of the Marine Corps Association & Foundation

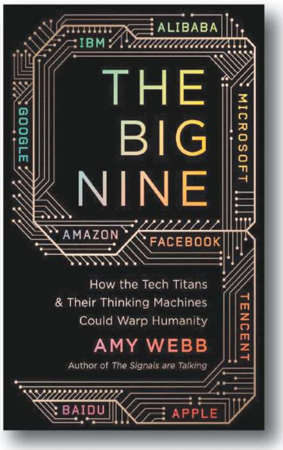


April 2020
Volume 104 Number 4

MARINE CORPS Gazette
Professional Journal of U.S. Marines

36 Cover Article
Effective C2 faces several challenges.
(Photo by PFC Ulises Salgado.)

DEPARTMENTS


ALIBABA
IBM
THE BIG NINE
GOOGLE
MICROSOFT
AMAZON
FACEBOOK
How the Tech Titans & Their Thinking Machines Could Warp Humanity
TENCENT
AMY WEBB
Author of The Signals are Talking
BAIDU
APPLE

IDEAS AND ISSUES

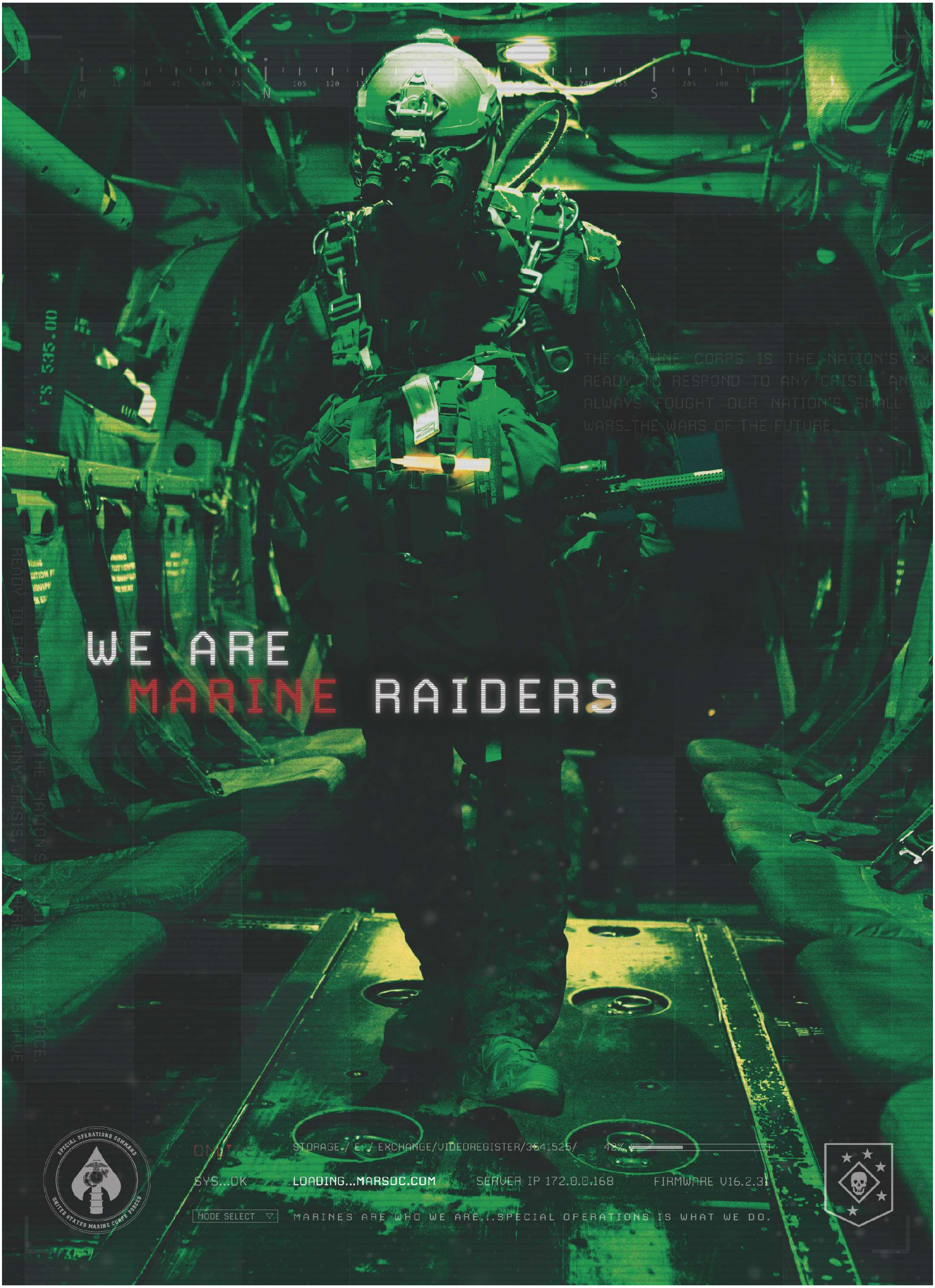
C4/OIE

Commentary

Leadership

Training

The *Marine Corps Gazette* (ISSN 0025–3170) is published monthly by the Marine Corps Association & Foundation to provide a forum for the exchange of ideas that will advance knowledge, interest, and esprit in the Marine Corps. Periodicals postage paid at Quantico, VA, USPS #329-340, and at additional mailing offices. • OPINIONS expressed herein are those of the authors and do not necessarily reflect the attitude of the Department of Defense, Navy Department, or Headquarters Marine Corps. "Marine Corps" and the Eagle, Globe, and Anchor are trademarks of the U.S. Marine Corps, used with permission. • MEMBERSHIP RATE: Annual $42.00 • MEMBERSHIP INFORMATION: Contact Member Services, 1–866–622–1775. • ADVERTISING QUERIES: Defense Related Industries/Business: Contact LeeAnn Mitchell, Advertising@mca-marines.org 703-640-0174. All other Advertising Contact James G. Elliott Co. Inc., Phone New York: 212-588-9200 Chicago: 312-236-4900 Los Angeles: 213-624-0900. • COPYRIGHT 2020 by the Marine Corps Association & Foundation. All reprint rights reserved. • EDITORIAL/BUSINESS OFFICES: All mail and other queries to Box 1775, Quantico, VA 22134. Phone 703–640–6161. Toll Free 800–336–0291. Fax 703–640-0140. Location: Bldg #715, Broadway St., Quantico, VA 22134. • E-MAIL ADDRESS: gazette@mca-marines.org. • WEB ADDRESS: www.mca-marines.org/gazette. • CHANGE OF ADDRESS: POSTMASTER: Send address changes to *Marine Corps Gazette*, Box 1775, Quantico, VA 22134 or e-mail: mca@mca-marines.org. • For credit card orders, call 866-622-1775. PUBLISHER'S STATEMENT: Publication of advertisements does not constitute endorsements by MCA&F except for such products or services clearly offered under the MCA&F's name. The publisher reserves the right to accept or reject any advertising order at his absolute discretion.



MARINE CORPS
ASSOCIATION & FOUNDATION
EST 1913

President & CEO
LTGEN W. MARK FAULKNER, USMC(RET)
www.mca-marines.org/gazette • 1–800–336–0291

Publisher, Editor, & Chairman, Ed. Adv. Panel
COL CHRISTOPHER WOODBRIDGE, USMC(RET)
c.woodbridge@mca-marines.org Ext. 163

Senior Editor
LTCOL KERRY A. KNOWLES, USMC(RET)
k.knowles@mca-marines.org Ext. 109

Layout/Editorial Production Coordinator
CHARLENE K. MONROE
c.monroe@mca-marines.org Ext. 139

Assistant Editors:
WILLIAM TREUTING
w.treuting@mca-marines.org Ext. 193

CARRIE EMERSON-COYLE
c.emerson-coyle@mca-marines.org

Administrative Assistant
HARLEY Q. PARKER-COLLINS
h.parker-collins@mca-marines.org Ext. 180

Advertising Queries:
Defense-Related Industries/Business:
Contact: LEEANN MITCHELL: 703-640-0174
Advertising@mca-marines.org
All Other Advertising Contact:
JAMES G. ELLIOTT CO. INC.
New York: 212-588-9200
Chicago: 312-236-4900
Los Angeles: 213-624-0900

MARINE CORPS
Gazette
Professional Journal of U.S. Marines

APRIL 2020

Editorial: Operations in the Information Environment

"Information overload" is an expression often used to describe the quantity and complexity of data and information converging on military planners and decision makers in today's world. Without a holistic understanding of all aspects of the information environment and a strategy for employing, protecting, prioritizing, and controlling this information, then a loss of competitive advantages and risks to the mission and to the force are clear. This understanding must include the interrelationship of those functions and systems traditionally grouped under the aegis term "C4I" (Command, Control, Communications, Computers, and Intelligence), and more broadly Operations in the Information Environment or "OIE," including the hardware/software networks and the electro-magnetic spectrum they depend upon. Moreover, the training and management of the Marines who operate in the environment and the purpose of the actual information being exchanged must also be understood. Whether conducting defensive cyberspace operations to protect information about friendly forces, attacking the physical network of an adversary to deny access to accurate information, or delivering truthful information to U.S. and allied publics, a comprehensive approach is essential to success in this complex environment.

"Information overload" could also describe the OIE-related content in this month's *Gazette*—fully twenty articles in print plus another ten featured online. However, beginning with a letter from LtGen Lori E. Reynolds, the Deputy Commandant of Information (DC I) on page 4, this month's series of articles all contribute to explaining the Corps' approach to understanding and managing the diverse aspects of operating in the information environment. In addition to the articles featured on this month's cover, I strongly endorse the following highlights to build a more complete understanding of OIE.

In "Marine Corps Information Operations Center" on page 9, Col Francis K. Chawk—the MCIOC Commander—provides an overview of his organization's role in military information support operations and military deception. On page 23, LtCol Dennis W. Katolin offers foundational definitions for the OIE in "Information Defined." Recognizing the broadly diverse set of activities that inform and influence the public, "The Power of Music" by Col Jason K. Fettig on page 29 describes the unique and invaluable contribution traditional military music makes in a comprehensive communications strategy and public information plan. Communications strategy is also the subject of "Who needs COMMSTRAT?" by Capt John J. Parry on page 52.

Linking the Corps' Warfighting philosophy to offensive and defensive cyber-operations is the focus of "Maneuver Warfare in the Cyber Domain" by Capt Joe McGinley on page 40. OIE and C4I encompass both the art of command and the science of communications. The art of establishing effective command relationships to support the Corps' future operating concept is the focus of "Command and Control Considerations for EABO" by Marc Riccio & Maj William Grimball on page 60, and the science of operating with degraded or denied communications is covered in both "Spectrum Contested Environments" by LtCol Christopher S. Tsirlis on page 71, and "ANW2 Expanded" on page 82 by Maj Adrian E. Ybarra, et al.

As always, critical discourse and constructive critiques are always welcome in the Corps' professional journal. Participate in the dialogue and access all the *Gazette's* content at www.mca-marine.org/gazette.

Christopher Woodbridge

MCA&F President and CEO, LtGen W. Mark Faulkner, USMC(Ret); *Chief Operating Officer*, Col Dan O'Brien, USMC(Ret); *Director Foundation Operations*, Col Tim Mundy, USMC(Ret); *Director of Strategic Communications & Editor*, Leatherneck *magazine*, Col Mary H. Reinwald, USMC(Ret); *Member Services*, Jaclyn Baird; *Chief Financial Officer*, Johnna Ebel.

Marines seek to own the operational environment. We plan, adapt, innovate, and train rigorously and realistically. When it comes time to fight, we are poised to outcycle the enemy because we understand the challenges and opportunities posed by the environment.

In today's interconnected world, we have to think beyond the physical environment. Narratives can travel the globe at a rapid pace, influencing governments and threatening or shoring up democratic processes. Our formations rely on navigation from satellites and can be targeted by the emissions from their equipment. A single user's carelessness on the network can provide an opening for hackers to take down our weapons systems. A single social media post can give away a unit's movements.

All of these components—the Internet and its infrastructure, the devices we use to communicate, our data, the narratives we share, the electromagnetic spectrum, the space and cyber domains—form a multi-layered and complex information environment. We live in the information environment all the time, and actions taken in the information environment can have physical effects. Just as we have done for 244 years, the Marine Corps will adapt to this new environment faster than anyone else to protect our nation, which is now under persistent attack.

To that end, the Commandant established information as a warfighting function in February of 2019. It is now up to us to understand information—how to both defend against it and leverage it to best impose our will on the enemy—and the new operating environment.

We own the battlespace when we're fighting in the air, on land, or at sea. We have to adapt so we can own the information environment, too. Adaptation requires innovation. The articles in this issue of the *Gazette* are meant to spark ideas and conversation. We need Marines of every rank and community engaged from competition through conflict; this is a fight for everyone.

Our challenge is to take these concepts and either find a way to operationalize them or counter them with a better idea. Through constant adaptation, rigorous preparation, and aggressive maneuver our Corps has established a formidable reputation and track record of success. With your help, we will continue to fight and win.

Semper Fidelis,

LEReynolds

L. E. Reynolds
Deputy Commandant for Information

The Race to Digitalization

How digitalization will revolutionize military capability and the seven strategies we need now to harness it

by Col John Shafer, USMC(Ret) & Charles Rath

The machinegun. The tank. The airplane. These technological innovations fundamentally changed the way wars have been waged. Those who ignored the technologies or failed to appropriately adapt to them were found to be ineffective and suffered disproportionate casualties.

Now, in the 21st century, digitalization—the convergence of big data, cloud computing, artificial intelligence (AI), and the Internet of things (IoT)—will be the single most transformative development that revolutionizes war more quickly and dramatically than ever before. Leaders of nations who invest in, appreciate, and ultimately embrace this movement will thrive. Those who fail to respond will never catch up and will rapidly lead their countries into being irrelevant or extinct. It is a scary proposition. But it is not up for debate.

The fundamental problem that commanders face—making the right decisions at the right time to achieve desired outcomes—has not changed since the time of Alexander the Great. Gaining and maintaining information dominance is key to timely decision making at the strategic, operational, and tactical levels.

The difference between Alexander's time and ours is in the speed, volume, platforms, and formats of the information—the data—to be processed. To be effective in the modern operating environment and make decisions at a faster pace than adversaries, whether facing peer competitors or non-state actors, our C2 architectures need assured, secure global access to data with mechanisms to identify, filter, and deliver information at the right time and in the right format for leaders to make appropriate decisions.

>Col Shafer retired after serving 37 years as an Infantry and Reconnaissance Marine. He commanded at every level from the platoon to the regiment, and he experienced five combat tours. In retirement, Col Shafer is the President of Centurion Solutions, a company that provides defense-related consulting services as well as serving as a site lead for Metris Global in Camp Lejuene, NC.

>>Mr. Rath is the President & CEO of RS21, a data science and visualization company that leverages insights from data to empower people to make data-driven decisions. He has more than fifteen years of experience as a global resilience expert and brings unique expertise in the field of resilience and risk management, having been in leadership positions in private, public, and national laboratory settings relating to this kind of work.

> ***The speed of modern military decision-making must exceed the speed of modern war.***
>
> ***—Gen Joseph Dunford***

Furthermore, the United States must be able to operate in denied, degraded, intermittent, and low-bandwidth (DDIL) environments, as well as master and dominate the data realm to compress the decision-making process. Masterfully merging all data interfaces and developing and refining algorithms is the best way to outpace adversaries and maintain a strategic advantage.

DOD officials have wrestled with the digitalization challenge for some time and have yet to achieve the objective of big-data management. But the ability to integrate different data sets then analyze and deliver them in understandable, applicable formats is at our fingertips. To truly embrace and invest in digitalization, the key will be to partner with the private sector to transform reams of data which have long been catalogued but have become too cumbersome to mine into actionable insights.

The private sector has been most affected by digitalization, and nowhere is the adaptation toward this trend more evident than in business. Nearly 50 percent of the Fortune 500 companies listed at the turn of the century are no longer relevant. It is estimated that 40 percent of companies currently on the list will be extinct in 10 years.

Behemoth corporations, long known for strength and dominance, are being upended by small, agile companies whose leaders are smarter, faster, and far more capable of disrupting traditional industries.

The same trajectory is feasible for today's global warfighters. Who can forget Russian President Vladimir Putin's ominous quote: "Whoever becomes the leader within this sphere [AI] will become the ruler of the world."

Data Deluge

Ninety percent of the world's data was created in the last two years. This data comes from satellites, sensors, cell phones, and nearly every electronic gadget. It creates opportunities to understand our world in ways that were inconceivable just a few years ago. The source of this data is known as the IoT. But we always had a lot of data. What is so different now?

Rapid developments in cloud computing allow the capability to crunch and store massive amounts of information. Processing terabytes and petabytes of data is no longer novel and is actually considered quite pedestrian in the Information Age.

AI makes it possible for machines to learn from experience, adapt to new data, and perform human-like tasks. Machine learning models quickly sift through massive amounts of data in order to identify trends, make predictions, and inform transformative decisions.

Opportunities

How will convergence of big data, cloud computing, IoT, and AI transform the military? Some areas have advanced more than others, but below are a handful of game-changing examples. Let's examine them through the lens of the six classic Warfighting Functions:

Intelligence. In the traditional sense, development of the collection plan has been a time-consuming task which usually completely relies on intelligence assessments deduced from human interpretation across multiple sources usually spanning a prolonged period of time. This data is then painstakingly evaluated and compiled, and a collective assessment—made by humans—is applied. Many times these assessments are informative and accurate, but arguably more times they are not, because lengthy processing time considerations and human factors introduce error probability. Now in the age of digitalization, we can create an interface that allows for assessment of collective data, spanning all collection sources over a predetermined time horizon most reflective of current operational considerations. This interface can then instantaneously run those unrestricted data sets against multiple algorithms to determine the most likely and most dangerous enemy courses of action with a high probability of certainty, all in minutes, not weeks. This is intel driving operations.

Maneuver. The U.S. military has preferred methods of maneuver. Our doctrine seeks to pit our strength against our opponents' weaknesses at the appropriate time. Regardless of domain, this approach offers few options to those exercising the offense. Our doctrine has been studied extensively by our adversaries. There are only so many ways one needs to defend against our maneuver. However, our doctrine also states that maneuver is intended to exploit an opponent's weakness. Imagine removing the uncertainty in determining exactly where the adversaries' weaknesses actually are? Data collection and realtime analysis combined with data visualization can predict where enemy exploitability and gaps do and will exist.

Fires. Long range, indirect, and air and surface delivered fires are essential for success on the modern battlefield. Technology has come a long way in creating "smart" munitions, which can deliver fires exactly where you want them. This has greatly enhanced warfighter capability, however, it falls short of where we could be. Today's precision fires do only one thing—deliver fires to an exact location. What they do not do is tell you exactly when and where you want them. Imagine a combined fires system that not only delivers pinpoint accurate fires but also delivers those fires at the right time, in the precise location, achieving desired effects on the target while virtually eliminating the concern of collateral damage. Battlefield target and engagement data, combined with environmental and collateral factors continuously analyzed through AI algorithms, can deliver complete fires solutions at the time of need—accessible from the requesting unit level to the fires releasing authority level—simultaneously.

Logistics. Just in time logistics? Forward logistics depots or "iron mountains?" No more. Image data analytics, from the smallest to the largest units, visually and understandably depict who requires what, when, where, how, and why, and informs the appropriate agencies and systems to deliver those requirements at the right time and place via the most secure methods and routes.

Force Protection. AI can provide realtime information at the individual, unit, and platform level that can pinpoint friendly locations and integrate into fire control systems to eliminate blue-on-blue engagements by overriding human weapons employment decisions. Enemy tactics, techniques, and procedures and partner force behavior patterns can be analyzed to develop predictive models that can be utilized to inform mitigation strategies, greatly reducing surprise engagements.

C2. AI algorithms and machine learning can improve and eventually perfect decision making by placing the human *on the loop* as opposed to relying on the human to be *in the loop*. Imagine an environment with a system that compiles, analyzes, and makes sense of all available, relevant data and conveys that to the human decision maker. And this all occurs at the appropriate time, combined with mission parameters and requirements, to provide a clear, relevant, complete, feasible, suitable, and acceptable course of action—all ahead of an adversary and faster than the speed of war.

The Seven Key Components of a Sound Digitalization Strategy

The sheer scale of change required to establish global digital superiority is tough to comprehend. Where do we start? Following are seven practical ideas for every organization in the DOD to consider while transitioning from the past to the present and future:

People. As companies, research institutions, and governments race toward innovation in AI and smarter everything, one profession has risen above all else: data science. Competition is fierce. LinkedIn recently reported a shortage of 151,717 people with data science skills in the United States. The median sal-

NEXTGENERATION

ary for a data scientist is $185,000 per year. Currently, there are limited career paths for data scientists at the DOD. But even if there were more opportunities, Department officials would have a hard time winning the war on talent. To compete, leaders must embrace out-of-the-box personnel models in order to attract brain power to join their ranks. DOD's Chief Data Officer Michael Conlin suggests a "public-private talent exchange" as a way to capture top talent who want to make a difference. This is certainly the type of approach that's needed. Given the supply and demand of talent, DOD officials must embrace non-traditional partnerships with innovative industry partners if they want to rapidly move the needle and sustain it.

Non-traditional partnerships. In order to access the Nation's most disruptive companies, DOD leadership must overhaul traditional acquisition strategies. During the time that traditional defense contractors make a push toward digitalization capabilities, they will be challenged to keep up with smaller, more agile companies that are capable of innovating at the speed of technology. Continued use of other transaction authorities that are not encumbered with tedious and prohibitive guidelines will be central to keep pace with emerging technologies and capabilities.

Cloud computing. In his insightful book, *Digital Transformation: Survive and Thrive in an Era of Mass Extinction,* Thomas Siebel highlights elastic cloud computing as the essential foundation of moving toward digitalization. In short, cloud computing enables organizations to crunch massive amounts of information in parallel sequences at once. For example, cloud computing would allow the military to process and understand millions of disparate data from the battlefield at the same time. Cloud computing's infinite capacity and rapid elasticity make it essential for the DOD's digitalization strategy.

Data integration. The problem of "data silos" in the DOD is well documented and understood. Efforts are well underway to solve the problem of structured data integration. However, the ability to seamlessly integrate and derive insights from structured *and* unstructured data is key. Structured data is what everyone studied in statistics class, such as birth dates and phone numbers, and is usually stored in easy-to-understand databases. Integrating unstructured data (everything else) is where magic happens. Unstructured data can be anything from satellite imagery to cell phone location data, and from sensors to photographs. The ability to integrate all this information—*and derive meaning from it*—will allow military leaders to exponentially increase their intelligence and agility in the battlefield and beyond.

Modern software development. Modern software development methods are quite possibly the least sexy attribute of digitalization to talk about at cocktail parties, especially approaches that allow military officials to harness agility and flexibility in the face of rapid technical advancements. However, it may be the most unnoticed but most important attribute. Traditional approaches to software development at the DOD render the organization incapable of adapting to emerging trends. However, using containers—an open source software development concept that securely packages software and all its dependencies for use across multiple computing environments—is a game changer for the military. Containers dramatically speed up development time while allowing the DOD to quickly and effectively switch out components to meet specific mission needs.

Usability. A major general at the Association of the U.S. Army Conference in downtown Washington, DC, expressed her frustration:

> Even when we can get our arms around all of the data, it's impossible to understand—there's just too much of it.

The fields of human-computer interaction and user experience design were created to help the human mind easily process digital information. However, these experts are rarely consulted when big data applications are developed. The result? Big, nasty interfaces that no one understands or wants to use. Integrating designers as part of the development team can drastically increase the likelihood of success. In fact, incorporating user experience research into traditional development cycles can yield a return on investment of between 10-100 times.

DDIL functionality. DDIL environments are omnipresent and should be anticipated in all DOD operations. To no one's surprise, emerging technologies tend to work seamlessly in impeccably clean environments with high-speed Internet service and armies of programmers and tech teams to immediately resolve problems. However, transitioning that capability to the battlefield is significantly more challenging. Researchers and practitioners must build digitalization strategies and networks that make data access and computing assured regardless of the degree of DDIL challenges encountered.

To seize transformational moments, we must embrace out-of-the-box, disruptive solutions. Granted, this can be hard to find in traditional bureaucracies. These solutions must be driven by foundational principles and frameworks that create a united effort across government, industry, and the research community leadership.

The world is at a pivotal moment in modern military history. The pace of technological innovation is so rapid that it nearly defies imagination. Those who harness it will reign supreme. Those approaches that allow militaries to harness agility and flexibility in the face of rapid technical advancements may be the most unnoticed, but most important attributes. Traditional approaches to software development at DOD, for example, tethered the agency to outdated technologies and vendors, rendering the organization incapable of adapting to emerging trends. However, by working with the most innovative companies and leveraging the most cutting-edge technologies, the DOD can dramatically speed up development time to quickly and effectively switch out components to meet specific mission needs. True digitalization is a game changer for the military and DOD.

Marine Corps Information Operations Center

Past, present, and future

by Col Francis K. Chawk, III

>Col Chawk is a MAGTF Intelligence Officer and Planner. He began his career as a Ground Intelligence Officer with 3d Battalion, 5th Marines. Also a Foreign Area Officer for Western Europe and a Regional Affairs Officer for the Middle East and North Africa via experience, he became an Advanced IO Planner before assuming command of MCIOC in 2018.

The Marine Corps Information Operations Center (MCIOC) was originally established under the Deputy Commandant for Plans, Policies, and Operations with the release of *MARADMIN 266/09*, *Establishment of the MCIOC*, in April 2009.[1] Two years later, in February 2011, *MARADMIN 094/11* announced that MCIOC had reached full operational capability.[2] MCIOC has been described well in several previous articles: see then-Capt Emily Grant's *Gazette* April 2010 article[3] and Otto Kreisher's *Leatherneck Magazine* article from December 2010[4] for reference. With the establishment of the Deputy Commandant for Information (DC I) in 2017, MCIOC transitioned from Plans, Policies, and Operations to DC I along with what were then the Intelligence and the Command, Control, Communications, and Computers Departments. A colonel has led MCIOC since its creation. Originally a "director," the first board-slated colonel assumed command of MCIOC in 2012.

The purpose of this article is to share with readers what MCIOC does now and what the future holds for the center. Well beyond the scope of this article, this is not a discussion or debate on information operations versus operations in the information environment. *Suffice it to say, the Corps has adopted operations in the information environment (OIE) as the construct for future employment, and the term "IO" will be phased out.* This could eventually lead to a name change for MCIOC itself, but a name is not what matters for the Corps or deployed forces. What matters are the capabilities that deployed units and Marines need to operate successfully now and in the future.

***Gen "Big Lew" Walt.** (File photo.)*

The Marine Corps defines OIE as:

> Actions taken to generate, preserve, or apply military information power in order to increase and protect competitive advantage or combat power potential within all domains of the operational environment.[5]

The term OIE is *not* simply a replacement for IO. OIE consists of seven functions and six capability areas (see Figure 1 on next page). It is critical that as the Corps transitions to OIE, Marines do not claim, "Yeah, I know … It's all really just IO," because, quite simply, it's not. All MAGTF officers should learn and gain an appreciation for these functions and capability areas. Understanding these functions and capabilities will be increasingly important and will support what Marines do as fighting forces.

Located on the west side of I-95 in Walt Hall named in honor of Gen "Big Lew" Walt, the first four-star assistant commandant of the Marine Corps, MCIOC provides support to MARFORs, MEFs, MIGs, deploying MEUs, SPMAGTFs, and other organizations with subject matter experts, teams and detachments, and psychological opera-

Seven Functions of OIE	Six Capability Areas of OIE
1. Assure enterprise C2 and critical systems.	1. Electromagnetic spectrum operations.
2. Provide info environment battlespace awareness.	2. Cyberspace operations.
3. Attack and exploit networks, systems, and info.	3. Space operations.
4. Inform domestic and international audiences.	4. Influence operations.
5. Influence foreign target audiences.	5. Deception operations.
6. Deceive foreign target audiences.	6. Inform operations.
7. Control OIE capabilities, resources, and activities.	

Figure 1. OIE functions and capability areas.

tions (PSYOP) Marines. In addition, the center maintains relationships with several sister Service and Joint organizations. MCIOC coordinates with Training and Education Command on the current MOS producing courses used to designate Marines as 0510, 0550, and 0551.

MCIOC's current strength is just slightly more than 200 personnel on hand. While active duty Marines make up the bulk of that number, the center has government civilians, a small Individual Mobilization Augmentee (IMA) detachment, and contract support as well. In addition to the headquarters element with the CO, chief of staff (civilian), XO (lieutenant colonel), and sergeant major, the center is broken down into two subordinate companies: headquarters (HQ Co) and PSYOP. While both are led by majors, the two companies are vastly different.

HQ Co

In HQ Co, MCIOC has the standard staff sections that one would expect to find in a Marine command: S-1, S-2, S-3, S-4, and S-6. In addition, the center has an S-8 (which will be discussed below), security, procurement, budget, and several other key sections. Nearly all the sections are made up of a mix of active duty Marines, government civilians, and contract support, augmented at times by Marines from the IMA detachment.

The S-3 is the largest and most diverse section within HQ Co and is led by a lieutenant colonel with a government civilian as the deputy. In addition to overseeing unit and individual annual training, readiness reporting, global force management requirements, lessons learned, and a variety of other tasks, the S-3 also oversees and directs three regional support teams (RSTs) that provide reach-back support for the MCIOC Marines who are forward deployed with MEUs, SPMAGTFs, and filling joint requirements. Led by government civilians, these three RSTs are roughly ten personnel each and have a mix of government civilians, officer and enlisted Marines, and contract support. RST 1 focuses on the Middle East, RST 2 has the Pacific and South America, and RST 3 focuses on Europe and Africa. MCIOC and the RSTs have recently begun to reach out to the supported units preparing for deployments to inform those units what reach-back support the RSTs can provide them while they are forward deployed and highlight the capabilities that the center provides in general. Within the S-3, and the RSTs in particular, MCIOC has several billets for officers completing their foreign area officer or regional affairs officer payback tours after completing their coursework at Naval Postgraduate School (NPS). Naturally, these RSTs have constant interaction with the MARFORs and MEFs/MIGs which share their areas of interest.

The S-3 section also oversees the publicly available information cell and the Marine operations security team (MOST). The publicly available information cell supports operations through input to the RSTs and the MOST conducts operational security assessments of Marine units per Marine Corps Order 3070.2A.[6] MCIOC S3 is currently assessing the MOST's role with DC I and ways to "operationalize" operational security assessments to review physical, technical, and administrative signatures.

In addition to unit and individual training, the S-3 section also has a small S-37 section which focuses on information related training that MCIOC provides to Marines, sister Services, and international partners. Previously known as the Combined Unit Exercise, MCIOC has run a two-week training evolution aboard MCB Quantico for several years. That exercise generally consisted of a week of staff training, followed by a week of practical application in a field environment—complete with a variety of scenarios, role players, leaflet drops, and limited use of information related gear and equipment. MCIOC is assessing how and where it conducts this training and the current plan is to evolve the name to the Information Warfighter Exercise with a continued focus on influence and deception operations, but with the ability to incorporate all functions and capability areas of OIE.

Perhaps somewhat unique to MCIOC, the center also has an S-8 section which works a diverse portfolio of new gear and equipment, input to doctrinal and concept employment, future requirements, MOS development, and other initiatives. In this capacity, the S-8 works on a regular basis with Marine Corps Warfighting Laboratory, Combat Development and Integration, Total Force Structure Division, and others. The S-8 also oversees the newly created signature management platoon. Like the S-3, the S-8 section is also led by a lieutenant colonel with a government civilian as its deputy. This section is typically where NPS graduates with the 8834 (Technical Information Operations Officer) and 8866 (Space Operations Officer) FMOS complete their NPS utilization tours.

PSYOP Co

PSYOP Co is naturally where the majority of MCIOC's 0521 (PMOS) and 0522 (secondary MOS (SMOS)) PSYOP Marines reside. 0521 became a PMOS with the release of *MARADMIN 343/18* in June of 2018.[7] Currently, 0522 remains a secondary MOS for enlisted Marines who remain in their PMOS, but 0522 will be phased out as the Corps grows several hundred 0521s across the Corps over the next several years. For officers, 0520 is the secondary MOS for those who complete the PSYOP qualification course at Fort Bragg and additional courses at Virginia Beach, VA. In addition to *MARADMIN 343/18*, DC I recently released *MARADMIN 690/19* in December 2019 to continue to advertise the opportunities and requirements for Marines interested in careers in the PSYOP field.[8] Marines who are interested should discuss this with their career counsellor and consider making the move to this growing field.

PSYOP Co focuses on the training and subsequent employment of PSYOP Marines who deploy in support of operational requirements. As previously stated, these requirements are prioritized at Marine Forces Command through the global force management process. On a continuous basis, PSYOP Co has nearly 50 percent of its Marines either forward deployed, in some stage of training, temporary additional duty in preparation for deployment, or in dwell. Marines who return from deployments often serve in the RSTs or in the S-3 so that their recent operational experience can feed into the support that the operations section provides to the next rotations going forward. PSYOP Marines who are up for PCS orders are currently starting to rotate out to the Fleet Marine Forces for assignment within the newly created PSYOP sections within the MIGs. With a small handful of PSYOP Marines at each MIG, current focus of effort is to increase the MIGs' capacity over the next several years. MCIOC's PSYOP Co also has a small detachment of communication strategy Marines who assist in graphics on PSYOP production efforts.

The Future

As mentioned, all three MIGs will eventually have their own, organic PSYOP sections. Originally envisioned as two companies (one on the east coast and one on the west), the current structure (based on Future Force 2025 growth) will be less than 35 PSYOP Marines at each MIG. As the structure comes on-line for those billets and as the Corps lateral moves, trains, and PCS Marines into the MIGs, those MIG Marines will take on the tactical-level requirements that MCIOC Marines have filled for more than a decade. This will drastically improve work relationships and ease deployment requirements that MCIOC has filled. Currently, if a MCIOC Marine is going to support a deploying unit out of Okinawa, California, or North Carolina, that Marine and his or her team could join the unit several months before the deployment for work-ups, followed by the actual deployment itself, and then any follow-on requirements that may arise at the tail end of the mission. This could easily turn a six-month deployment into nearly a year away from home station (Quantico). While this may seem like a standard "price of providing support," it can be very costly in terms of temporary additional duty and time away from families when that support comes from Quantico. Conversely, there are times when a MCIOC Marine does not join the deploying unit until days or weeks before deployment because of unavoidable circumstances. That situation nearly always equates to a less than ideal construct because of the lack of integration with the deploying unit. In the future, when the support comes organically from Okinawa, Pendleton, and Lejeune, with the gear and equipment they need to operate, support relationships to those tactical-level units will undoubtedly improve.

Marine Corps Information Operations Center logo. *(Logo provided by author.)*

However, one caveat from the writer's perspective is that the Marine PSYOP sections within the MIGs will most likely not be enough to meet all the requirements for each MEF. MCIOC has seen that with MOS training timelines, school throughput, slight yet unavoidable attrition at schools, PME requirements to keep Marines competitive for promotion, and other factors, it often takes "three to make one." With the recurring missions of MEUs, SPMAGTFs, and other requirements, I argue the MIGs will need to continue to grow their PSYOP sections, particularly if the demand for 0521s continues to increase over time. If the MIGs are capped with the Marine PSYOP sections, they will see a continuous deployment-to-dwell cycle of 0521s, which could lead to exhaustion and burn out. The MIGs, MCIOC, and Manpower Management Enlisted Assignments will need to be aware of the operational tempo and monitor its effects on PSYOP Marines. Without a doubt, Marines who laterally move to PSYOP will have multiple opportunities to deploy in support of operational requirements.

In theory, once the MIGs have reached full operational capability and are able to sustain the tactical-level requirements, MCIOC's focus will shift more to the operational level. Already working at this level as well, MCIOC currently supports MARFORs and several joint task forces with planning expertise, subject matter expert exchanges, operation plan development, and other tasks. That will continue and expand as MCIOC pulls out of the tactical level over the next three to five years. MCIOC will continue to serve as the Service's center for expertise with an initial focus on influence and deception operations while continuing to build relationships with those units and commands who focus on electro-magnetic spectrum, cyber, space, and inform operations. By doing so, MCIOC will continue to evolve from a command that was focused on influence and, to a lesser extent, deception to a command that will be involved in all seven functions and six capability areas for OIE.

Working with all capability areas for OIE, MCIOC's role in training and preparing units for deployments will also likely increase. Already working with Marine Corps Tactics and Operations Group at Twentynine Palms, Marine Corps Cyberspace Warfare Group, MAGTF Staff Training Program, and Training and Education Command, the center is assessing how and where its cadre of expertise could help continue to drive OIE into all training in which Marine units participate. MCIOC has supported and will continue to support Weapons Tactics Instructor, TBS, EWS, Command and Staff, the School of Advanced Warfighting, and others with presentations and subject matter expert support. Because MEFs will want their MIGs to be tested and evaluated during training, perhaps experts from MCIOC will be able to expand the training role that currently exists to develop that capability further. MCIOC will also serve as the center for lessons learned so that experience gained by one MIG can be shared with the others to increase the learning cycle and advance concepts faster.

Throughout this evolution, MCIOC will continue to provide input on doctrinal development, conceptual employment of OIE, design of future gear and equipment, and other Service-level requirements that will require input from MCIOC's experienced staff. Ideally, Marines who have completed tactical-level information related tours with MEFs, MarDivs, MAWs, MLGs, and the MIGs will at some point serve on the MCIOC staff where their experience will inform and shape doctrine, policy, and future concepts. Of course, the Marines who are not 0521s will have to ensure that they maintain proficiency in their PMOSs. Back-to-back information related tours could potentially be detrimental to a Marine's career, unless the Corps were to consider an information occupational field.

Information Occupational Field (Occfield)?

It is worth noting that every additional or free MOS for officers doing a tour in the information field (0510 intermediate MAGTF IO practitioner, 0520 PSYOP, 0530 Civil Affairs, 0540 Space, 0550 Advanced MAGTF IO planner, 8834, 8866, etc.), all remain secondary MOSs. This poses multiple challenges. First, there is an obvious training timeline and pipeline that officers must go through in order to have a basic understanding of the billets in which they will serve. Training and education can range from courses lasting two weeks (0510) to two years at NPS (8834, 8866). Additionally, it means that the vast majority of the officers serving in information related billets could be doing their job for the first time. MCIOC currently has officers whose PMOSs include 02XX, 0302, 0402, 0802, 1302, 3002, 6002, 6602, 7204, 7208, 7315, and 7565. While this is tremendous for the broad skillset it brings to the officer cadre on the MCIOC team, it means that officers come to MCIOC with a varying degree of familiarity and experience in the information field. The final challenge is that all officers will PCS from MCIOC (or any other information related billet in the fleet) and go back to their PMOS for their next assignment. While many may desire to continue to work in the information field, the current Marine Corps system requires Marines to maintain proficiency in their PMOS. Otherwise, their chances of continued promotion, and therefore continued service, could be limited. This applies to all enlisted Marines as well, except for those who lateral move to 0521.

With the creation of information as a joint function,[9] and the Marine Corps' subsequent adoption of information as a warfighting function,[10] perhaps the Corps should consider what it would take to create an information occfield. As previously noted, all officer additional MOSs and free MOSs in the information field remain *secondary* MOSs. If the Corps—Manpower Management Officer Assignments in particular—were to assess 0510, 0520, 0530, 0540, 0550, 8834, 8866, and other MOSs, there may be enough structure to create an information field. That occupational field, along with intelligence (02XX/26XX), communications (06XX), and cyber (17XX), would all remain core elements within the DC I hierarchy. With a three-star lieutenant general DC I advocating for those fields, the potential to integrate and advance all seven functions and six capability areas within OIE would have tremendous opportunity for growth and improved support to deploying Marine units.

While heretical to some and even frightening to others, the author also believes that the Communications Strategy and Operations (CommStrat) field (45XX) should be considered for that occupational field as well. While seemingly sacrilegious to consider PSYOP and CommStrat Marines working side-by-side in the same field, that is exactly what the information field needs to create a force capable of operating in the environment envisioned by the *Commandant's Planning Guidance*.

Conclusion

The MCIOC has served the Corps well for the past decade and will continue to evolve, particularly as the requirements to operate in the IE continue to increase. Developing technologies, operational concepts, and capable pacing threats will demand that all Marines, not just those working in the information field, consider and debate how Marine units are structured and resourced for the future challenges they will face. If the Corps truly embraces that information is the seventh warfighting function, perhaps the Corps should consider careers in that field and how those opportunities could expand and improve the support that MCIOC provides to the Service.

Notes

[1] Headquarters Marine Corps, *MARADMIN 266/09, Establishment of the Marine Information Operations Center*, (Washington, DC: 2009).

2. Headquarters Marine Corps, *MARADMIN 094/11, MCIOC Full Operations Capability*, (Washington, DC: 2011), available at: https://www.marines.mil.

3. Emily Grant, "The Marine Corps Information Operations Center," *Marine Corps Gazette*, (Quantico, VA: April 2010).

4. Otto Kreisher, "Information Operations: Developing a Marine Corps Capability," *Leatherneck Magazine*, (Quantico, VA: December 2010).

5. Deputy Commandant, Combat Development and Integration and Deputy Commandant, Information, Joint Memorandum, "Definition for Information Related Terms," (Washington, DC: January 2020).

6. Headquarters Marine Corps, *MCO 3070.2A, The Marine Corps Operational Security (OPSEC) Program*, (Washington, DC: July 2013).

7. Headquarters Marine Corps, *MARADMIN 343/18, Announcement of Psychological Operations (PSYOP) 0521 Primary Military Occupational Specialty and instructions for Lateral Move*, (Washington, DC: June 2018).

8. Headquarters Marine Corps, *MARADMIN 690/19, Solicitation of Qualified Marines for Lateral Move into the Psychological Operations Primary MOS 0521 and Release of FY 20 Schedule for Psychological Operations Screening and Assessments,* (Washington, DC: December 2019).

9. *Joint Publication 1* Extract with CH-1 states, "The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant actor perceptions, behavior, action or inaction, and human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides JFCs the ability to integrate the generation and preservation of friendly information while leveraging the inherent informational aspects of all military activities to achieve the commander's objectives and attain the end state." (Washington, DC: July 2017).

10. Headquarters Marine Corps, *Marine Corps Bulletin 5400 (MCBUL 54), Establishment of Information as the Seventh Marine Corps Warfighting Function*, (Washington, DC: January 2019), available at https://www.marines.mil.

Information and Uncertainty

New forms of conflict are possible

by Eric X. Schaner

>Mr. Schaner works in the Information Plans and Strategy Division (IPS), Deputy Commandant for Information (DC I), HQMC.

The subject of information has drawn interest and debate for millennia. Information is as old and ingrained in the human experience as is the written word. Information is well defined in science, mathematics, and engineering to serve as the basis of applied communication theory. Given the change in the nature of the modern global security environment—due in large part to the way information and modern global digital communications have changed this environment—it is necessary to discuss information from three related military perspectives: the signal-substance of all forms of communication, an instrument of national power, and the seventh Marine Corps warfighting function. This article discusses information from these perspectives using *uncertainty* as a connecting theme.

What Is Information?

The world in which we live is most often described in terms of mass, velocity, and other physical attributes. However, a quantity as important as these and vital to understanding the nature of our surroundings is *information.* Whether we consider computers, biological systems, physics, artificial intelligence, the human brain, or opposing nation states and military organizations, we are driven to conclude their behaviors largely depend on the way they process information.[1]

Information is precisely defined in mathematical terms as a binary digit, or "bit." This simple term provides the basis of applied communication theory, and in turn the basis of all man-made and biological forms of communication. However, within the Marine Corps we commonly use the term *information* generically to refer to all manner of descriptions and representations from raw signals to knowledge and understanding.[2]

To make the most effective use of information, an expanded understanding of it is required. Whether applying information theory in communications and engineering endeavors, or more broadly in military competition and war, the unifying theme of information is that in all cases it refers to a *reduction of uncertainty as a result of the ability to discriminate useful signals from noise.*

These useful signals convey meaning with a value proportionate to the degree uncertainty is reduced. If the signal does not reduce uncertainty, the signal is noise. If the signal misleads or deceives the recipient, the signal is *misinformation or disinformation*. Simply, information reduces uncertainty, whereas misinformation or disinformation increases uncertainty—or increases certainty of a falsehood.

Referring to information as a signal discriminated from noise that reduces uncertainty is useful in the military context. Focusing on the concept of *uncertainty* as the common theme of information helps to explain both information as an instrument of national power and information as the newest Marine Corps warfighting function.

How we share and process information is important. **(Photo by LCpl Joshua Sechser.)**

Information as an Instrument of National Power

Information is one of the four instruments of national power, with the other three being diplomatic, military, and economic. These instruments refer to the resources available to a nation to achieve national strategic aims. These resources are available during times of cooperation, competition, and war.

Information is an instrument of national power because *information is power.* This adage derives from the Industrial Age where information provided competitive advantage to a nation with superior *know-how* in leveraging value-producing resources—typically land, labor, capital, and material resources such as minerals.

While information was important in the Industrial Age, it is *existential* in the Information Age. This change stems from the dependency advanced societies now have on information and the never-ending revolution in information technologies and global digital communications that define the post-industrial era. With dependency comes potential vulnerability, and with vulnerability comes potential advantage to the side seeking to exploit the vulnerability.

To understand potential vulnerabilities associated with information dependency, we look no further than societal institutions such as banking, health care, manufacturing, transportation, energy, trade and commerce, and all governmental functions. These institutions depend on databases and advanced computing systems and algorithms simply to function. This marks a significant change from the Industrial Age when these institutions functioned manually with physical-manual means of data storage, processing, and communication.

Additionally, the connection people have with these institutions is increasingly dependent on digital communications, to include the Internet, mobile communications, and data applications. Our world has become digital and networked, providing adversaries with virtually unlimited ways to interfere with an institution's data or the means of communicating with these institutions.

ELEVENTH MARINE EXPEDITIONARY UNIT
PRIDE OF THE PACIFIC
11TH MARINE EXPEDITIONARY UNIT
#CARATBRUNEI2019
#FREEANDOPENINDOPACIFIC
U.S. Marines and Sailors joined Royal Brunei Armed Forces for Cooperation Afloat Readiness and Training Brunei, where both forces trained in urban and jungle environments to enhance interoperability and partnership between the U.S. and Brunei.

How do we use social media? ***(Photo by LCpl Jared Sabins.)***

Another feature of information dependency is the degree to which people use the Internet, social media, and digital communications to socially interact, plan, and coordinate activities, and receive news and information. The unending trend of accelerated technology development will increase the dependency people have on digital communications and social media technologies to exchange information, socially interact, and interpret their environment. This introduces another critical vulnerability where aggressors may seek to manipulate information flowing through social networks and other media to alter a person's social reality and perception of truth.[3]

Because of the information dependencies noted above, the informational instrument of national power becomes increasingly important in the Information Age. The consequence of information dependency is the opportunity it affords aggressors to manipulate vital information to increase the *uncertainty* people have with their institutions, thereby altering their perception of truth. The United States should employ a comprehensive strategy through the informational instrument of national power to build resiliency against potential aggressors in the information environment. This leads to a discussion of information as a warfighting function.

Information as a Warfighting Function

Societal information dependency is a vulnerability shared by Information Age militaries. During the Industrial Age, U.S. technological superiority contributed to global reach and relative information superiority. This superiority was characterized by the numerous ways in which information about a threat could be gathered, processed, and exploited to some effect, such as bringing combat power to bear at a specific time and place anywhere on the globe.

The inherent assumption during the Industrial Age was that information

How we conduct OIE can affect the utilization of our combat forces. ***(Photo by SSgt Patricia Morris.)***

contained within intelligence, command and control, communications, and weapons systems was largely secure, accurate, and trusted. *The Information Age has fundamentally undermined this assumption and thus altered the technological and combat power advantages the United States experienced during the Industrial Age.*

Because the Marine Corps is an Information Age military organization, it is as susceptible to information manipulation or denial as are other advanced societies. Competitors and adversaries alike understand our information dependency, and we should expect them to exploit it to foil our ability to function—regardless of how much combat power we attempt to muster.

To increase our capacity for competing and fighting in the Information Age, the Marine Corps in January 2019 established information as the seventh warfighting function. This action followed the establishment of information as the seventh joint function in July 2017.

The new warfighting function provides a framework for the commander and staff to integrate information into all operations. More specifically, the information warfighting function provides a framework that solidifies a Service perspective recognizing the necessity of information by making information *generation*, *preservation*, *denial*, and *projection* the commander's business.

From this overarching framework, the Marine Corps is developing derivative concepts and terminology such as *Military Information Power* and *Operations in the Information Environment* (OIE) to describe how information generation, preservation, denial, and projection achieves advantage in competition and war. Military Information Power was established as a term in a joint memo signed by the DC I and the Deputy Commandant for Combat Development and Integration in January 2020. This term is described further in a currently proposed Marine Corps Doctrinal Publication on Information. Operations in the Information Environment was also established as a term in the January memo. This term will be expanded upon in detail in an intended Marine Corps Warfighting Publication on OIE.

Underpinning these emerging concepts and terminology is leveraging information for competitive and combat power advantage. The theory is simple and goes like this: through the information warfighting function framework the Marine Corps plans and conducts OIE to create and leverage military information power for competitive and combat power advantage. Military information power creates advantage over an opponent by increasing their uncertainty, increasing their certainty of a falsehood, or by denying them the information needed to function. This is accomplished through information generation, preservation, denial, or projection. Military information power is discussed in more detail in the article entitled "What is Military Information Power?" within this issue (on page 17).

Conclusion

Significant changes in the global security environment are driven in many ways by changes in the nature of information and the never-ending revolution in information technologies and global digital communications. Because of these changes, new forms of conflict are possible such as the targeted deceptive messaging of individuals or groups within a society, and the denial of vital institutional information to cause societal disruption. Information Age militaries suffer the same vulnerabilities of information dependency as do advanced societies as a whole. While information has always been important, it is now existential for the effective functioning of military organizations. The joint force and Marine Corps are adapting to this new environment by developing new functions to serve as a framework for commanders to integrate information in all operations and focus the use of information to create competitive and combat power advantage.

Notes

[1] James V. Stone, *Information Theory: a Tutorial Introduction,* (Sheffield, UK: Sebtel Press, 2016).

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

[3] Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, and Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment*, (Santa Monica, CA: RAND, 2019).

What is Military Information Power?

The post-industrial information environment

by Eric X. Schaner

>Mr. Schaner, see page 14 for bio.

Information has long been understood and employed as one of the four instruments of national power. Information, along with the diplomatic, military, and economic instruments of national power encompass the total resources available to the Nation. These resources are employed to achieve strategic objectives and the policy aims which encompass the national interest. This article draws from the classical notion of the informational instrument of national power and changes in the post-industrial information environment to derive a theory of military information power.

The Theory of Military Information Power

The global, instant, and persistent nature of information in the post-industrial era has reshaped the global security landscape. This new era, sometimes called the *Information Age*, creates opportunity for aggressors to directly target the underlying data and networks of information required for the effective functioning of societal institutions. This is possible due to the dependencies in institutions such as banking, health care, manufacturing, transportation, energy, trade and commerce, and all governmental functions now have digital data as well as advanced computing algorithms and networks to provide their services.

The Information Age also creates opportunity for aggressors to directly target individuals and groups of individuals to feed them misinformation or disinformation in order to alter their perception of reality. This is possible because of the degree to which people rely on the Internet, social media, and digital communications to socially interact, plan and coordinate activities, and receive news and information.[1]

A recent RAND study refers to the above phenomena as characteristic of a new form of conflict called *virtual societal warfare.* This form of conflict is executed by aggressors through a combination of attacks on critical societal-institutional data and targeted deceptive messaging through traditional media and social media to alter peoples' social reality and perception of truth.[2]

The growing trend of societal information dependency and the subsequent vulnerabilities is an issue shared by Information Age militaries—including the Marine Corps. During the Industrial Age, technological superiority firmly established the United States as the world's sole military superpower. A defining feature of superpower status was the assured access to and use of information to bring combat power to bear anywhere on the globe.

We can no longer assume combat power overmatch as a result of assured access to information. America's peer competitors are developing capabilities to directly target the data and underlying networks of information the United States currently relies upon to generate and employ combat power. Peer competitors are also challenging United States influence and partnerships through the employment of gradually coercive ambiguous activities, backed by aggressive

Peer competitors are also challenging United States influence and partnerships through the employment of gradually coercive ambiguoius activities. *(Photo by Cpl Nathan Reyes.)*

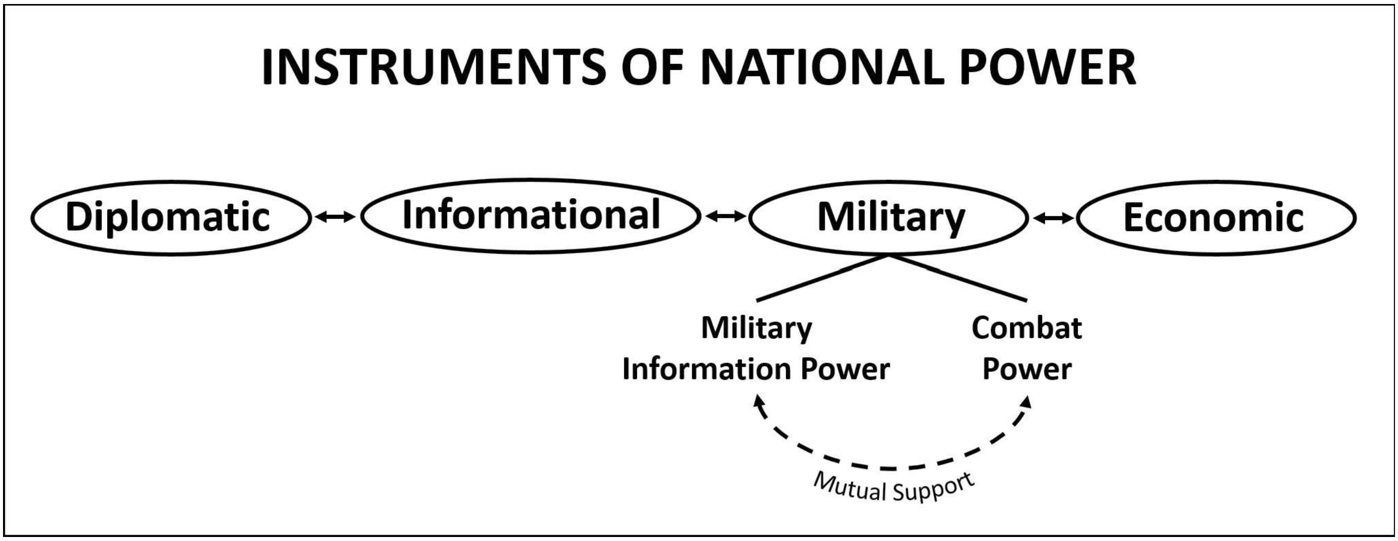


Figure 1.

narratives and propaganda. This type of challenge deliberately remains below the threshold of armed conflict to avoid a traditional U.S. military response.

This leads to a *theory of military information power*. The theory is an expanded view of the military instrument of national power such that it comprises two mutually reinforcing elements—*combat power* and *military information power*. (See Figure 1.)

According to joint doctrine, combat power is defined as "the total means of destructive and/or disruptive force that a military unit/formation can apply against the opponent at a given time."[3] The U.S. military projects combat power in armed conflict or general warfare. To expand upon the concept of combat power, the Marine Corps recently issued a joint memorandum to define the term military information power. The memorandum was signed by the Deputy Commandant for Information and the Deputy Commandant for Combat Development and Integration in January 2020.

The memo defined military information power as:

> the total means of force or information capability that can be applied against a relevant actor to enhance lethality, survivability, mobility or influence.[4]

The memo established the term as official interim guidance to inform doctrine development. This new term underpins expanded thinking about the military instrument of national power and its applicability across the competition continuum.

Military information power is broadly applicable in competition and war, and it is a necessary mutually supporting element to combat power. The side with the ability to manipulate, deny, or destroy the information required for the decision making and basic functioning of the opposing military system, while preventing the opponent from doing the same, achieves significant advantage—including a combat power advantage. *The essence of military information power is the ability to exert one's will or influence over an opponent through the generation, preservation, denial, or projection of information.*

Information preservation refers to building resiliency to the dependencies and vulnerabilities we have on information and the digital communications required to compete and win in battle.

Information Generation

Information generation refers to the preparatory activities conducted to increase our competitive potential in the information environment, such that we may exploit this advantage to achieve some effect in any operational domain. Activities include analyzing the information environment from a threat, friendly, neutral, and physical environment perspective; planning and preparing specific courses of action; gaining the authorities to execute specific actions; and gaining access to the opponent's information environment—to include databases, communications networks, social networks, key leaders, and trusted influencers.

Information Preservation

Information preservation refers to building resiliency in the dependencies and vulnerabilities we have on information and the digital communications required to compete and win in battle. Information preservation involves activities such as implementing strong cybersecurity measures; conducting defensive or offensive cyberspace operations, or physical attack to protect our

MILITARY INFORMATION POWER

Information Generation	Information Preservation	Information Denial	Information Projection
• Analyze Information Environment • Develop Courses of Action • Gain access to opposing Information Environments	• Cybersecurity • Defensive Cyberspace Operations • Spectrum Management • Signature Management • Counter-propaganda	• Cyber-attack • Electronic attack • Directed Energy • Physical attack • Operations Security • Signature Management	• Radio Broadcast • TV broadcast • Social Media • Print media • Cellular communications • deception

Note: The above table does not provide a definitive list of the ways and means of military information power. It is up to the commander and the creativity of the staff to devise ways of maximizing advantage using all available resources.

Figure 2.

networks; effectively managing the use of the electromagnetic spectrum; and exercising effective operations security and signature management. It also involves building resiliency to negative news, propaganda, and narratives—to include social media narratives—that work against our mission and objectives. This requirement is increasingly a primary concern for commanders at all echelons.

Information Denial

Information denial describes the use of any means available to gain advantage over an opponent by denying them vital information. This may include manipulating, disrupting, or destroying the information needed by the opponent to sense, make sense, and act. Active information denial involves activities such as cyberattack, electronic attack, directed energy attacks, and physical attack to name a few. Passive means of denying the opponent vital information may include selectively altering or suppressing the physical and digital signatures emanating from friendly forces. This may also include implementing operational security measures, communications discipline, camouflage, and strong cybersecurity measures.

Information Projection

Information projection refers to transmitting information of any type to inform, influence, or deceive an observer—such as the people, government, or military of a competitor or enemy nation. The Marine Corps may project information in many ways to include direct communications such as radio, television broadcast, print media, cellular communications, and social media. Information may also be projected by taking physical actions knowing they are observable, and by knowing what informational impact such actions may create. The methods and objectives of information projection should always be considered with information denial.

Figure 2 depicts and summarizes the elements of military information power as combination of information *generation*, *preservation*, *denial*, and *projection* based on the discussion above.

Conclusion

The theory of military information power provides the theoretical foundation for a more practical discussion of how the Marine Corps generates, preserves, denies, and projects information to gain advantage and achieve objectives. To accomplish this, the Marine Corps has been advancing the concept of operations in the information environment through the establishment of the MEF Information Group. The MEF Information Group is a formation at the tip of the spear in operationalizing the theory above into practice across the whole of the MAGTF.

Notes

[1] Michael J. Mazarr, Ryan Michael Bauer, Abigail Casey, Sarah Anita Heintz, and Luke J. Matthews, *The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment,* (Santa Monica, CA: RAND, 2019).

[2] Ibid.

[3] Joint Staff, *Joint Publication 3-0, Joint Operations, incorporating Change 1,* (Washington, DC: October 2018).

[4] Joint Staff Joint Memorandum, *Definitions for Information Related Terms,* (Washington, DC: HQMC, January 2020).

What are OIE?

Definition and functions

by Eric X. Schaner

In January 2020, the Marine Corps issued a joint memorandum to officially define two new terms: *military information power* and *operations in the information environment* (OIE). This article discusses the definition of OIE and its associated "seven functions" in the context of military information power.

OIE

The Marine Corps began developing concepts and implementing organizational changes in July 2017 to build capability and capacity for OIE. As the Corps continues to evolve OIE, new guidance emerged in the January memo. This guidance included a formal definition of OIE as:

> actions taken to generate, preserve, or apply military information power in order to increase and protect competitive advantage or combat power potential within all domains of the operational environment.[1]

The definition establishes a direct link between OIE and the new term military information power. The Marine Corps, through the information warfighting function, plans and conducts OIE to create and leverage military information power for advantage. Military information power concerns exerting one's will or influence over an opponent through four primary OIE actions: *information generation, information preservation, information denial, and information projection.*

The Marine Corps envisions OIE to be persistently conducted in global campaigns throughout the competition continuum and during armed conflict. OIE are conducted to support naval, Service, combatant command, and joint force objectives in the information environment (IE), and across all domains. In all cases, Marine Corps OIE are planned and executed in accordance with the following seven functions/tasks:

>Mr. Schaner, see page 14 for bio.

- Assure enterprise command and control (C2) and critical systems.
- Provide IE battlespace awareness.
- Attack and exploit networks, systems, and information.
- Inform domestic and international audiences.
- Influence foreign target audiences.
- Deceive foreign target audiences.
- Control OIE capabilities, resources, and activities.

Assure Enterprise C2 and Critical Systems

The first OIE function is vital to information preservation by assuring the information contained within C2, intelligence, communications, and weapons systems is secure, accurate, and trusted. Assured information within these systems is what allows the Marine Corps to sense, make sense, and act with a higher speed, focus, and tempo than an enemy. Assured access to and trust in the information contained within these systems is also the basis of combat power generation. In the post-industrial era, an era sometimes referred to as the Information Age, the generation and projection of combat power is *dependent* on access to and trust in the information upon which weapons systems depend for their functioning. Advanced adversaries understand this information dependency and will attempt to exploit it to counter our traditional combat power advantages.

Succeeding in this function involves a wide variety of activities to include: network modernization, training, DOD Information Network Operations, defensive cyberspace operations,

We must ensure that information received and transmitted is secure, accurate, and trustworthy. *(Photo by Cpl Ashley McLaughlin.)*

Operational security is only one of several areas of concern within C2 systems. ***(Photo by Cpl Ashley McLaughlin.)***

operations security, signature management, and electromagnetic spectrum operations. In addition to the above, this function also involves coordinating physical attack against aggressors targeting friendly C2 and intelligence systems.

Provide IE Battlespace Awareness

The second OIE function is vital to information generation by providing understanding of threats, vulnerabilities, and opportunities within the IE. This function gathers and fuses disparate information about the IE into a single comprehensive understanding. Through the second function, a coherent picture of the IE is formed by integrating three perspectives: the *threat*, *physical environment*, and *friendly forces*. These three perspectives are fused, analyzed, and developed into a single estimate. The estimate, commonly referred to as the "information environment running estimate," is a continuous evaluation of the IE used to inform the overall understanding of the integrated operational picture. The IE battlespace awareness function therefore provides an information-centric view of the commander's battlespace.

Succeeding in this function requires the ability to gather, fuse, and analyze a wide variety of information. The intelligence process supports this function by providing an assessment of the IE. However, this function does not exclusively rely on the intelligence process. Rather, it fuses information about the IE from any source that may inform of threats, vulnerabilities, and opportunities.

> ***In the Information Age there is a continuous battle for information to include a battle or narratives and the truth.***

Attack and Exploit Networks, Systems, and Information

The third OIE function is vital to information denial by exploiting the opponent's information dependencies for the purpose of disrupting their ability to function or to deny them advantage. This function involves aggressive means to disrupt the opponent from within. There are two primary ways of thinking about this function. The first is from a technical perspective which focuses on accessing, manipulating, disrupting, or destroying the opponent's data and underlying networks of information needed to generate combat power. The second perspective is non-technical and includes actions such as gaining access to and manipulating or disrupting the human and social influencers who aid the competitor or opponent.

Succeeding in this function requires leveraging the targeting process and the effective application of limited resources to prosecute key nodes within the opposing military system. This function also requires an effective feedback mechanism which leverages any available means of observing the target and identifying the effects of the attack.

Inform Domestic and International Audiences

The fourth OIE function is vital to information projection by truthfully communicating with domestic and foreign audiences in order to build understanding and support for operational and institutional objectives. It also seeks to reassure friends and allies, and deter and dissuade adversaries. While this function is largely led and planned by the communication strategy and operations (COMMSTRAT) and civil affairs occupational fields, they are executed and supported by commanders, staffs, and Marines in addition to the COMMSTRAT and civil affairs capabilities.

Succeeding in this function requires knowing higher-level strategic guidance and the associated narrative that supports friendly operations. Perhaps the most important requirement of this function is the ability to rapidly and dynamically communicate truthful information to counter negative narratives, malign and propaganda activities. In the Information Age there is a continuous battle for information, to include a battle for narratives and the truth.

Influence Foreign Target Audiences

The fifth OIE function is vital to information projection and/or informational denial by directly communicating with or withholding information from a relevant foreign target audience in order to influence their perceptions, decision making, and ultimately their behavior.

This function is used to maintain desirable conditions for our presence or objectives, or to turn unfavorable conditions to our advantage. This function is most closely associated with classical "information operations" and involves the professionals and capabilities, to include special technical capabilities, from this community.

Succeeding in this function requires the ability to integrate and leverage all means of communicating, or denying communications, to a relevant observer. This includes leveraging traditional means of communication such as radio, television, and print media, as well as cellular communications and social media. It also includes understanding and leveraging the message we communicate through our *physical actions* and *activities*. This may therefore require coordination through targeting process, fires and maneuver, in a similar manner as Function #3.

Deceive Foreign Target Audiences

The sixth OIE function is vital to information projection as well as information denial. By directly communicating with or withholding information from a relevant foreign target audience, this function seeks to compel the opponent to act or not act in a manner favorable to friendly force objectives. This function differs from the influence function primarily in the intended effect and authorities required to execute the function.

Succeeding in this function requires the integration of physical actions with specialized capabilities using a whole-of-staff approach. It also includes understanding and leveraging the message we communicate through our physical actions and activities. This may therefore require coordination through targeting process, fires and maneuver, in a similar manner as Functions #3 and #4.

Control OIE Capabilities, Resources, and Activities

The seventh OIE function is vital to information generation, preservation, denial, and projection. It is through this function that OIE capabilities, resources, and activities are harmonized and integrated into all operations. Awareness, timing, and close coordination with all Marine Corps warfighting functions are critical to the effective execution of this function.

We must be able to deceive the enemy as to our whereabouts and future activities. ***(Photo by Cpl Cutler Brice.)***

Succeeding in this function requires an organizational structure that assigns a commander with responsibility for OIE. Just as GCE and ACE commanders command ground and air operations, and leverage decentralized feedback-control loops to create combined, coordinated, harmonizing effect, so too should a commander command OIE and leverage decentralized control. To accomplish this, the Marine Corps should consider establishing an Information Combat Element (ICE) and give the ICE commander a command center that gathers, fuses, and displays all aspects of OIE to inform command decision. Establishing an ICE as a fifth MAGTF element, responsible for the seven OIE functions, could resolve the sometimes conflicting and confusing command relationships currently experienced between the MEF Information Group and MEF staff.

The IE battlespace awareness function therefore provides an information-centric view of the commander's battlespace.

Conclusion

Operations in the IE are the evolution of competition and conflict in the Information Age. The Marine Corps is evolving its terms, forces, concepts, and doctrine to meet the challenges of post-industrial Information Age. While these new terms, concepts, and doctrine continue to evolve, OIE will be implemented by the Marine Corps in accordance with the seven functions noted above to create and leverage military information power for competitive and combat power advantage.

Note

[1] Joint Staff, *Joint Memorandum: Definitions for Information Related Terms,* (Washington, DC: HQMC, January 2020).

Information Defined

A whole of force approach

by LtCol Dennis W. Katolin

>LtCol Katolin is assigned to Plans and Strategy, Deputy Commandant for Information, HQMC.

With the establishment of information as a warfighting function, the Marine Corps has evolved to the modern operating environment. However, to apply this function, Marines must first understand what information is. To that end, this article will define the term information for Marines based on how it is used in our operations.

Information as a Signal

MCDP 6, Command and Control (C2), defines information as the "usable knowledge," which is a part of the information hierarchy.[1] This doctrinal publication expands upon that definition to give a clearer understanding of information at its most basic level.

Information is a signal that has meaning in some context for its receiver.[2] In this sense, information is a noun. Information is more than just simple isolated facts. Rather, it must be seen as part of a system that includes data, physical systems, people, and decision making. Ultimately, this system is used to present information to the right audience, and at a specific time and place to inform, influence, or deceive that audience in order to achieve an advantage over our adversaries.

While the Marine Corps' use of information can have a strategic effect, it is not synonymous with information as an instrument of national power. We view information as part of power projection, defense, and maneuver within an operating environment. We use information to enable the military component of national power. Information makes the military instrument of national power more versatile and useful to better complement the diplomatic, information, and economic instruments of national power. (See Figure 1.)

In order to maximize the usefulness of maneuver, we must consider maneuver in other dimensions as well.

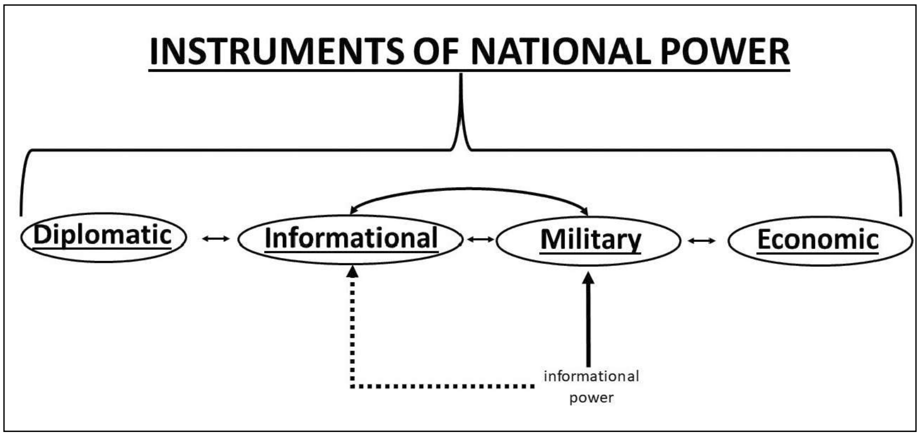


Figure 1. Information as part of the military instrument of national power.

This view of information is in keeping with our maneuver warfare doctrine of creating and exploiting an advantage over our adversaries. In fact, to truly apply maneuver warfare, we must think of every possible source of advantage over our adversaries. *MCDP 1, Warfighting*, states:

> In order to maximize the usefulness of maneuver, we must consider maneuver in other dimensions as well. The essence of maneuver is taking action to generate and exploit some kind of advantage over the enemy as a means of accomplishing our objectives as effectively as possible.[3]

Information as a Function

In addition to information as a signal, we also define information as a function. The function of information is performed to generate, preserve, deny, or project information to increase our advantage over the enemy. In this sense, information is a verb.

While the function of information involves the projection of signals, it also addresses actions that focus on information (the noun), cognition, and decision making. This can include physical and non-physical actions to deny, destroy, or manipulate their signals. As a result, the function of information must be viewed as a "whole of force" problem that requires a whole of force solution.

This also means—just as with every function in war—there is a symbiotic relationship with other functions. Given our expeditionary nature, Marines must appreciate the austere conditions that they operate in. Establishing technical information systems in such an environment will require maintenance and supplies (logistics) as well as knowledge of enemy threats to those systems (intelligence).

While the capabilities and sub-functions of information are addressed in the third chapter of *MCDP 6*, it is important for all Marines to understand that information must be seen as something we do. While we use information (the noun) to perform information (the verb), we have a broader scope of resources available to use to perform this critical function in war.

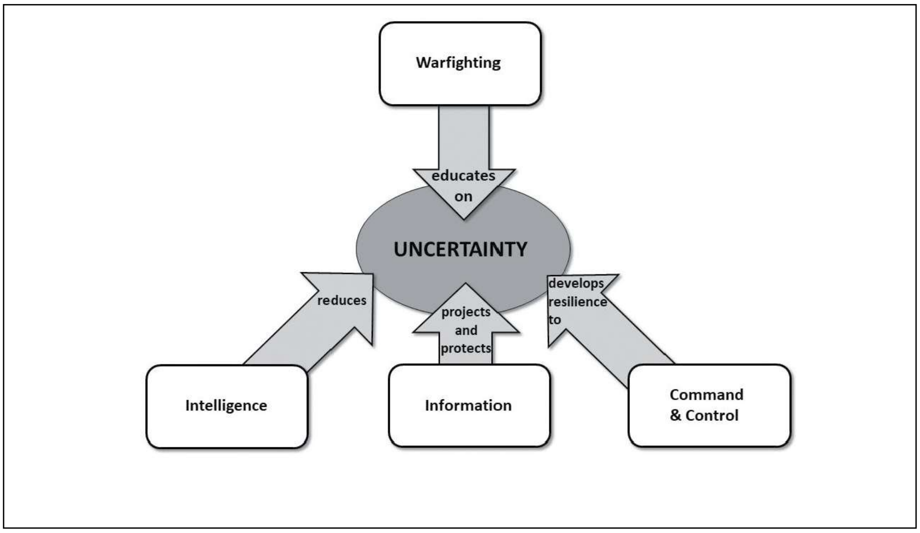


Figure 2. Information, intelligence, and C2 in relation to uncertainty.

Information, Intelligence, and C2

As we develop our understanding of what information is, we must be clear to differentiate it from what *it is not.* Information is not intelligence, or as *MCDP 2, Intelligence*, states, "intelligence is not simply another term for information."[4] *MCDP 6*'s information hierarchy shows information as the signal or raw data that leads to knowledge. This hierarchy makes information the foundational component to knowledge. When that knowledge tells us about the enemy or the environment, it is intelligence.[5]

We seek to either enhance or reduce uncertainty to impact the cognition and decision making of all relevant actors to influence their actions to our favor.

Nor is information the same thing as C2. As it is to intelligence, information is a vital part of C2. Information is one of the three elements of C2 along with people and support structure.[6] When information is used to represent the reality around us, it facilitates C2.

The question still needs to be answered, "what is the difference between information, intelligence, and C2?" The answer lies in their relationship to uncertainty. *MCDP 1* tells us that uncertainty is an inherent element of war's nature. With this knowledge, we seek to do three things in relation to uncertainty: we *reduce it*, we build *resilience to it, we project it.*

It is in these three objectives that we distinguish between the functions of intelligence, C2, and information. We use intelligence to reduce uncertainty by enhancing our knowledge of the enemy and the environment.

We use C2 to foster initiative and unity of effort while operating in the presence of uncertainty. In this sense, C2 builds our resilience to uncertainty by making the commander's vision clear and enabling the decentralized execution of our forces so they can adapt to an uncertain environment as they advance within it.

The function of information projects uncertainty. We seek to either enhance or reduce uncertainty to impact the cognition and decision making of all relevant actors to influence their actions to our favor. We may seek to create uncertainty in the enemy by saturating them with more information than they can process. We may want to enhance the enemy's certainty of what we are doing in an effort to deceive them. We may also want to reduce the uncertainty about us in our political leadership, the American people, or our partners and allies. The function of information also includes our efforts to protect ourselves from those that look to actively impose uncertainty on us.

While there is an inherently symbiotic relationship to the functions of information, intelligence, and C2, one should not simply say that they are the same thing. While information (the noun) is a necessary component of the function of either *reducing* uncertainty (intelligence) or *building resilience* to uncertainty (C2), the function of *projecting* uncertainty is distinct from the others and is now referred to as information. (See Figure 2.)

Information Age

Technology has always played a role in how we view the world around us. While boats have existed for millennia, the creation of submarines and aircraft carriers redefined naval power. Additionally, muskets were the primary weapon for centuries until the machine gun, which performed the same task as a musket but at a much more accelerated rate. This changed our approach to land warfare forever.

While information has always been a critical component of war, its importance has grown with the arrival of the information age. The information age occurred during the second half of the

20th century with the combined impact of the global Internet and the proliferation of affordable and highly capable information systems. This caused billions of people to access, generate, transmit, and consume information at a scope, scale, and speed that continues to accelerate exponentially beyond any other time in history.

Information has also impacted everyone's lives. The information age has allowed information's accelerated and expanded scope to impact militaries and societies from a distance and at a rate that has been unprecedented.

From digitally integrated fires across multiple domains from hundreds of miles away to the digital security, entertainment, and appliance systems in people's homes, the Information Age has allowed for a tremendously integrated and, consequently, a responsive world. The exponential proliferation of information technology has made information and the systems that generate, distribute, and present information a critical requirement for societal, military, and governmental institutions. As is the case with all powerful resources, information can be used for constructive or destructive means.

Given the rapid expansion of information's generation, transmission, and access, there is a tremendous opportunity for actors to effect other people and systems on a global scale. Consequently, an information environment has emerged, and we must understand how it has changed our operating environment.

Conclusion

Information is a critical component to success on the battlefield. It impacts our ability to understand the enemy, environment, and ourselves. Information enables our maneuver and ability to conduct combined arms faster and more effectively than our enemies. Marines must understand the nature of information and its relationship to people, time, and space in order to better understand how to access it, how it impacts us, and it can be projected to help us be successful.

Notes

[1] Headquarters Marine Corps, *MCDP 6, Command and Control*, (Washington, DC: 1997).

[2] This information is available at https://searchsqlserver.techtarget.com.

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

[4] Headquarters Marine Corps, *MCDP 2, Intelligence*, (Washington, DC: 1997).

[5] Ibid.

[6] *MCDP 6, Command and Control.*

The Nature of Information

Information is instantaneous

by LtCol Dennis W. Katolin

Once someone understands what information is, they must understand its nature. This is critical to the application of information as a function in war. This article will give Marines a better understanding of the nature of information in the Information Age, how we are vulnerable to it, and how we can leverage it in both conflict and competition.

Information Age and Environment

The information age has allowed billions of people to access, generate, transmit, and consume information at a scope, scale, and speed that continues to accelerate exponentially beyond any other time in history.

Given the rapid expansion of information's generation, transmission, and access, there is a tremendous opportunity for actors to effect other people and systems on a global scale. Consequently, an information environment (IE) has emerged, and we must understand how it has changed our operating environment.

The IE is the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information.[1] While it is not a warfighting domain (though it includes the warfighting domains of both space and cyberspace), it is a space that facilitates maneuver.

Global Reach and Perspective

Information is global. As the world becomes more and more connected, people will have the ability to disseminate information on multiple platforms throughout the entire world. The geographic boundaries we have grown accustomed to are instantly overcome or bypassed by information. Marines must think beyond the physical boundaries of their single battle construct, or even the geographic combatant command they are in. (See Figure 1.) Information has a global reach with potential global implications.

>LtCol Katolin see page 23 for bio.

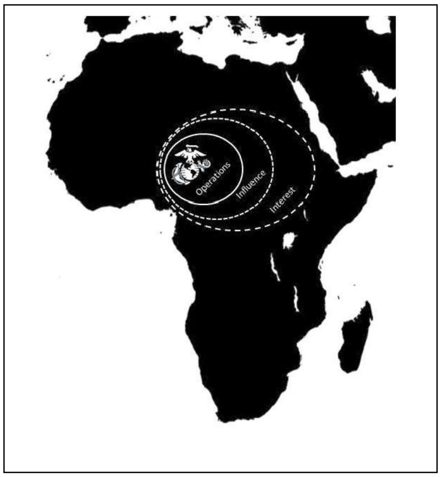


Figure 1. Traditional view of battlespace in the Industrial Age.

When we conduct operations, we must do so knowing that our ability to project information now has become global. Before our physical forces depart the continental United States, we can leverage information power to have effects on the enemy and influence with a global audience.

The global nature of information also means that we can receive information from global influencers. The previous paradigm of assessing adversaries' capabilities using "range rings" for indirect fires assets is no longer sufficient. We must understand that engaging a state actor in a certain location cannot narrow our awareness to just that specific adversary. Just as we think through the capabilities of the enemy on the battlefield in front of us, we must also consider the adversaries in the IE that are all around us. (See Figure 2 on next page.)

Information and Time

Information is instantaneous. The proliferation of personalized information systems allows thoughts, images, and products to bypass typical hierarchical organizational structure. The moment something happens or is created, it is instantly distributable. The IE is a "flat organization" that bypasses traditional supervisory or controlled distribution mediums. Regardless of the information's accuracy or lack of context, its immediate transmission can have global impacts on individuals or groups within social, military, and governmental organizations. This requires detailed anticipation and rapid responsiveness.

Our understanding of information, as it relates to time, is focused on the rate of transmission, the duration of its projection, and the delay of its effects. We must always ask ourselves: "How long will it take to send this information? How long will it be available? How long until it has the desired impact?"

Persistence

Information is persistent. Because of the global and instantaneous nature of

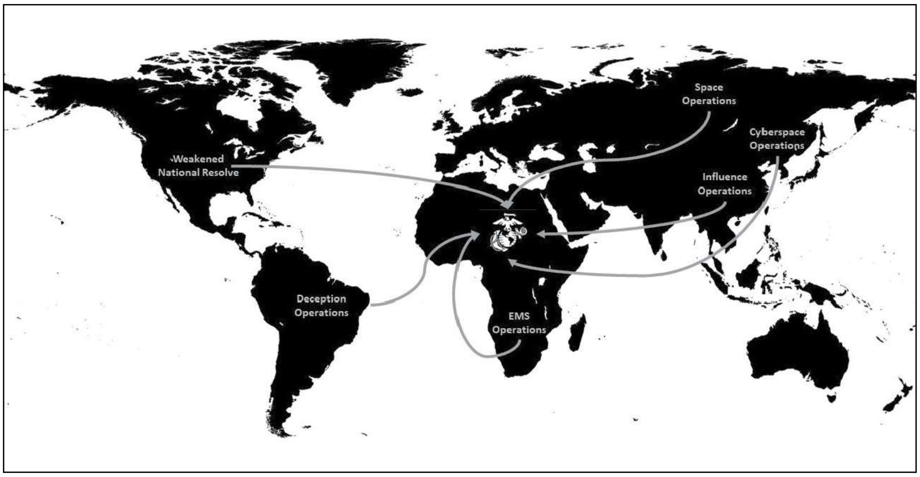


Figure 2. Redefined view of battlespace in the Information Age.

information, the Marine Corps must not culminate or take an operational pause in the IE.

The persistent nature of information challenges two existing paradigms we have about the beginning and ending of training and operations. The first paradigm to be challenged is the distinction between training and operating. The second paradigm to be challenged is the perception of when training and operating begins and ends.

With the emergence of the IE and the global, persistent nature of information, this distinction between training and operating has become blurred. Training events that access cyberspace, space, or spectrum are accessing contested space for information. Real-world adversaries will attempt to have real-world consequences for us as we train.

The persistent nature of information also means that there is no clearly defined beginning and end to our operations. There is no operational pause in the IE. Information's persistent nature requires a persistent presence and vigilance.

Information and the Levels of War

Part of our theory of war is that it consists of strategic, operational, and tactical levels. While the distinction of where one level begins and another begins is rarely binary, there often is an understanding of what levels of war one is operating at. This usually defines the scope and scale of what can impact us as well as how far the effects of our actions will reach.

Given the global, instantaneous, and persistent nature of information, we see an unprecedented compression of the strategic, operational, and tactical levels of war. While the relation of these levels have often shifted throughout conflicts, they have never been more closely linked than when we leverage information. (See Figure 3.)

Though Marines are often trained to think "two levels up" from their own units, we must now consider strategic context across geographic boundaries and consider how information generated from the tactical level in one side of the world.

Critical Thinking and OODA Loop Integrity

Credibility and accuracy are fundamental to ensuring that our actions are optimized to achieve our desired state. Misinformation can be used to cause us to orient on the wrong factors and will diminish our ability to focus combat power at the right place and time. As Sun Tzu says, "It is owing to his information, again, that we can cause the doomed spy to carry false tidings to the enemy."[2]

Critical thinking and reflection are necessary elements to determine what information we need and assessing if the information we have is credible. All information we consume must be scrutinized for its quality (credibility and accuracy).

This can be difficult in war as uncertainty is an inherent part of war's nature. Consequently, people will have a tendency to gravitate toward information in a desperate attempt to mitigate uncertainty.

The habitual practice of being reasonable, logical, and critical in thought helps us overcome the risk of emotional decision making. Critical thinking helps us to avoid cognitive shortfalls that compromise the quality of our decisions.

Information and the Trinity

In light of information's global and instantaneous reach, we must reflect on the inherent strategic implications of its reach. *MCDP 1-1, Strategy*, addresses Clausewitz's trinity consisting of the military, the government, and the national will of the people.[3]

These three pillars are vital to a nation's continuous ability to wage war.

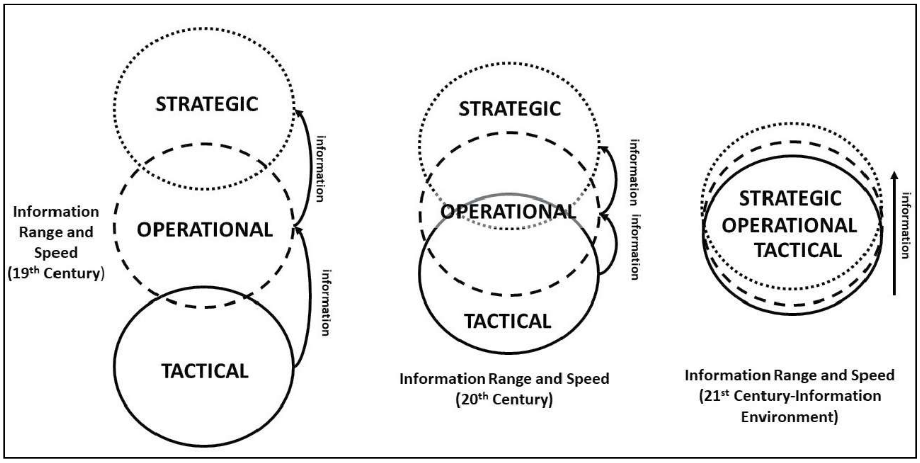

STRATEGIC
information
OPERATIONAL
information
TACTICAL
Information Range and Speed (19th Century)
STRATEGIC
information
OPERATIONAL
information
TACTICAL
Information Range and Speed (20th Century)
STRATEGIC
OPERATIONAL
TACTICAL
information
Information Range and Speed (21st Century-Information Environment)

Figure 3. Information's compression of the levels of war.

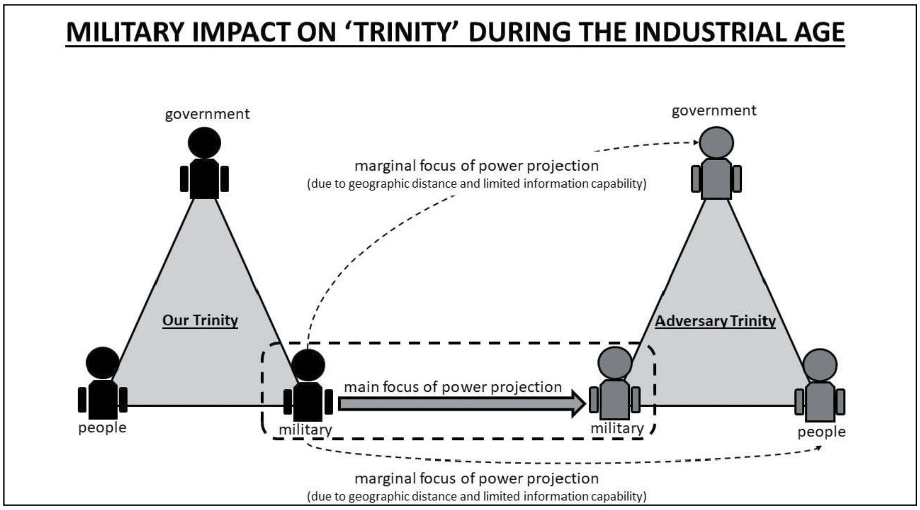

MILITARY IMPACT ON 'TRINITY' DURING THE INDUSTRIAL AGE
government
government
marginal focus of power projection
(due to geographic distance and limited information capability)
Our Trinity
Adversary Trinity
main focus of power projection
people
military
military
people
marginal focus of power projection
(due to geographic distance and limited information capability)

Figure 4. The Trinity in the Industrial Age.

Should one of these three pillars falter, a nation's ability to fight is compromised. At the strategic level of a war, a nation may focus the instruments of national power against any or all these three pillars.

In the Industrial Age of war, belligerents traditionally focused on defeating the nation's military pillar of war. Once the enemy's military capability was negated, that country's government and people were left vulnerable and were compelled to meet the terms of their adversary. (See Figure 4.)

Compelling a political decision is the objective of war. The defeat of the enemy's military is a means to that end.

In the Information Age, however, belligerents have the ability to directly target the government and people of an opposing nation to influence their decision. This can be done through conspicuous messaging and attacking information infrastructure used in everyday life. It can also be done through subtle and more indirect methods that impact people's cognition subliminally. (See Figure 5.)

Information is a critical component to success on the battlefield and impacts our ability to understand the enemy, environment, and ourselves.

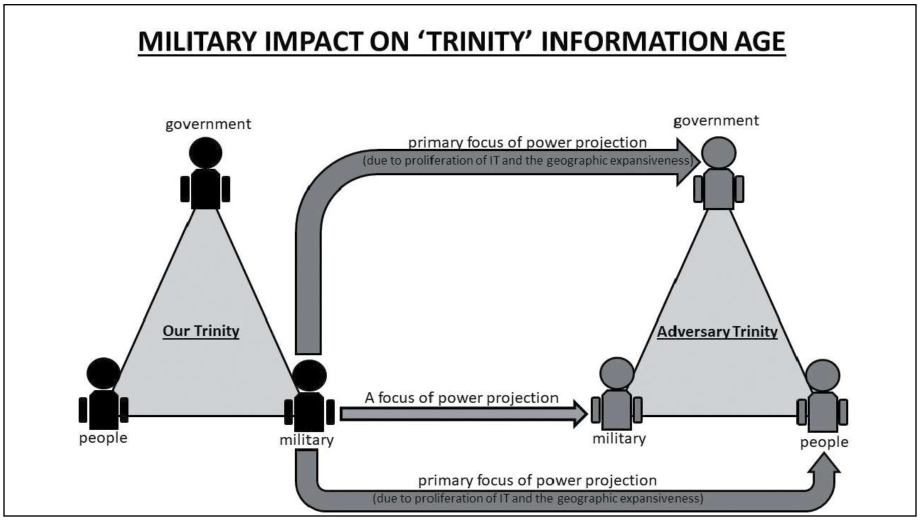

MILITARY IMPACT ON 'TRINITY' INFORMATION AGE
government
government
primary focus of power projection
(due to proliferation of IT and the geographic expansiveness)
Our Trinity
Adversary Trinity
A focus of power projection
people
military
military
people
primary focus of power projection
(due to proliferation of IT and the geographic expansiveness)

Figure 5. The Trinity in the Information Age.

While defending against the reach of the enemy's information, our own leaders must seek to exploit the reach of our information on the enemy. The ability to reduce, or bypass all together, the enemy's military to achieve political ends is the application of maneuver warfare at the strategic level. Bypassing the nation's strategic "surface," (their military) and exploiting their strategic "gaps" (government and people) allows us to focus power with minimal expenditure of resources.

Conclusion

Information is a critical component to success on the battlefield and impacts our ability to understand the enemy, environment, and ourselves. Information enables our maneuver and ability to conduct combined arms faster and more effectively than our enemies. Marines must understand the nature of information and its relationship to people, time, and space in order to better understand how to access it, how it impacts us, and it can be projected to help us be successful.

Notes

1. Joint Staff, *Joint Publication 1-02 (JP 1-02), The Department of Defense Dictionary of Military and Associated Terms,* (Washington, DC: 2010).

2. Tzu, Sun, *The Art of War and Other Classics of Eastern Philosophy*, (San Diego, CA: Canterbury Classics, 2016).

3. Headquarters Marine Corps *MCDP 1-1, Strategy*, (Washington, DC: 1997).

The Power of Music

Moving the Marine Corps forward

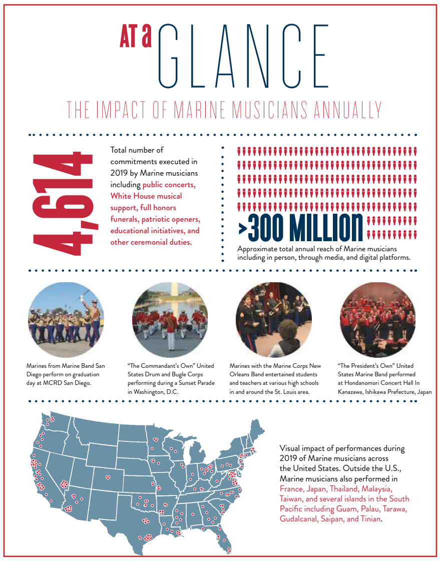
by Col Jason K. Fettig

>Col Fettig is the 28th Director of "The President's Own" United States Marine Band located at Marine Barracks, Washington, DC. He is the Music Adviser to the White House and regularly conducts the Marine Band and Marine Chamber Orchestra at the Executive Mansion and at all Presidential Inaugurations and State functions, as well as leads the band in performances all across the Nation each year. Prior to becoming the director, he was the Executive Officer and enlisted Musician in the Marine Band.

On 11 July 1798, President John Adams signed an Act of Congress that permanently re-established the United States Marine Corps and began the development of our heritage as the Nation's premiere naval expeditionary force. Embedded in that Act of Congress outlining the structure of our fledgling Corps was a provision for 32 drummers and fifers, along with a drum major and fife major prescribed to lead them. This collection of new Marine musicians would soon evolve into what is today known as "The President's Own" United States Marine Band. This Act set in motion a tradition of music that has been interwoven into the very fabric of our Corps for more than two centuries.

On its surface, music may not seem to be essential to the core warfighting mission of Marines; however, that Congressional action clearly allotted a substantial portion of the original force to the specialized service of musicians, and the initiatives of our earliest Commandants tell us why. At the behest of President Thomas Jefferson, Commandant William Ward Burroughs sent his officers on an international recruiting mission to find highly trained musicians to staff the early Marine Band. Music was the primary tool to demonstrate the high standards of the new force to potential recruits and was essential to encouraging the necessary support of a skeptical public. The tradition of music in those early days was not just used to move troops on the battlefield and in ceremony, although that was an important function; it also possessed the power to communicate the emotion inherent in the independent spirit of the Nation. Music moved people to serve, motivated the support of those who did not serve, and, perhaps most importantly, connected those in the fight with all those for whom they fought.

Much has changed and evolved in our Nation and in our Corps since 1798, but the fundamental values and standards of excellence that were established by our earliest generation of Marines have been passed along through the centuries. The music provided by Marines since our founding continues to proudly illuminate them.



Total number of commitments executed in 2019 by Marine musicians including public concerts, White House musical support, full honors funerals, patriotic openers, educational initiatives, and other ceremonial duties.

Approximate total annual reach of Marine musicians including in person, through media, and digital platforms.

Marines from Marine Band San Diego perform on graduation day at MCRD San Diego.

"The Commandant's Own" United States Drum and Bugle Corps performing during a Sunset Parade in Washington, D.C.

Marines with the Marine Corps New Orleans Band entertained students and teachers at various high schools in and around the St. Louis area.

"The President's Own" United States Marine Band performed at Hondanomori Concert Hall In Kanazawa, Ishikawa Prefecture, Japan

Visual impact of performances during 2019 of Marine musicians across the United States. Outside the U.S., Marine musicians also performed in France, Japan, Thailand, Malaysia, Taiwan, and several islands in the South Pacific including Guam, Palau, Tarawa, Gudalcanal, Saipan, and Tinian.

The music provided by Marines during one year. ***(Image provided by author.)***

Gen David H. Berger has set the Marine Corps on a new path toward further modernization and strategic focus on five critical pillars designed to make our Corps stronger, leaner, and evermore skilled. Our 38th Commandant has directed that "we must communicate with precision and consistency, based on a common focus and unified message." Communication of our values and goals will always be an essential component of our collective success in every area of performance on and off the battlefield, and music can—and will—continue to play a vital role in moving our Marine Corps forward.

Warfighting

Marines are an elite warfighting force with a strong naval heritage. Understanding our rich history as warriors during both times of conflict and times of peace informs the future capabilities of the force, and music has always been central in communicating those stories. During times of war, Marine Corps bands spread out across the Nation not only to rally the support of both major influencers and the American public but to also viscerally remind them of those who are in harm's way. In some cases, those very same musicians have put down their instruments and deployed alongside their brothers and sisters to join the fight.

Marines are known as the "first to fight," but they are also often the first on scene to assist in emergencies or contain a brewing crisis. Our Corps' long history with the Department of State and its expeditionary nature suits the Service well to support the goal of deterrence. As much as Marines are prepared for war, the primary goal will always be peace through strength and diplomacy. Time and again since the founding of our Nation, music has been the most powerful public tool of soft power and diplomacy, encouraging the support of allied nations, building coalitions, and celebrating cultural exchanges as the centerpiece of our collective strength.

Music directly supports theater security cooperation. It can enable commanders worldwide to engage with publics and local governments in creative and meaningful ways that traditional instruments of theater security cooperation might not allow. From symbolically representing our Nation in the most sensitive diplomatic environments to executing joint performances with our foreign counterparts both on our soil and abroad, the fundamental and constant presence of music in our Marine Corps extends a warm and welcoming hand across borders and cultures wherever possible, from the halls of the White House all the way to the most unstable and dangerous corners of the globe.

Force Design

As the Commandant leads the effort to maximize the effectiveness of our assets and modernize the force where needed, he reminds us that *people* are our most important asset and that "everything starts and ends with the individual Marine." Every force structure change will depend on the abilities and health of our Marines and the support they receive from both inside and outside of the Corps. The proliferation of music in the Marine Corps is central to this latter effort: putting Marines in full focus for all those we encounter. Just as the goal of our foundational naval integration is to ensure we can reach any clime or place at any time to meet our adversaries, our ability to *represent* that capability to the American public through the communicative and universal nature of music is not only very powerful, it is necessary. Music is a vital tool in the overall communication strategy of shaping the public's view of Marines and, equally important, the further potential and relevancy of the Marine Corps in the future operating environment.

People from all backgrounds often draw their impressions from emotions and symbolic gestures. Those emotions can drive critical decisions. When a President, member of Congress, or an everyday citizen personally interact with Marine musicians, they receive a specific storyboard of emotion that can frame the impression of the entire force. The most important identity of that force is a combination of our long and storied heritage seamlessly combined with the capacity for constant innovation and adaptability. The very essence of military music continues to be the perfect representation of our fundamental identity and a vital strategic asset to capture and reinforce that messaging for audiences of the widest possible range of backgrounds and views.

Harkening back to the earliest days of the Corps, music is still at the tip of the spear in building the future of the Marine Corps. When prospective recruits hear and see "The President's Own" perform for them in their small town, witness "The Commandant's Own" Marine Drum and Bugle Corps play to thousands on an elite international drill field, or watch one of the ten exceptional Marine field bands stationed at major commands throughout the Corps bring incredibly diverse music and engagement to local communities, they are very often moved to be a part of that same culture of excellence. Quite simply, talent attracts talent, and the immediate impact of music on inspiring each generation of Marines to join this elite Corps has been borne out time and again on Marine Corps Recruiting Command's total force and the Musician Enlistment Option Program missions. If people are the Marine Corps' number one asset, there remains no greater tool to bring those people to the fight.

Education and Training

As with our naval expeditionary forces, not all Marine musical units need to be identical, and indeed the Corps' musical capabilities have been adapted and shaped by our evolving needs. While each Marine musician is a highly trained expert in their field, the ten field bands, the Drum and Bugle Corps, and "The President's Own" Marine Band each continually expand the skillsets of their units to meet the mission and continually broaden the modes of outreach to meet the needs of the service as we modernize.

Talent management is central to this effort and, since recruiting, nurturing and keeping talent is a priority for the Commandant, the music field provides an ideal model for the rest of the Corps in this area. By the very nature of this occupational field, it is entirely staffed by well-trained and disciplined professionals who demonstrate a never-ending quest for improvement and expansion of skills. As the premiere musical unit of the Marine Corps, "The President's Own" in particular attracts and retains the most elite and highly educated musicians the Nation has to offer who specifically choose to enter the Service with their unique talents. Nearly 100 percent possess a bachelor's degree in the field, with more than 60 percent holding master's degrees, and over 15 percent achieving doctorates. The Drum and Bugle Corps is the only active Drum Corps in the Armed Forces and remains an exceptionally prestigious career field for specialists in this area. Along with the Drum and Bugle Corps, the more than 500 Marines who serve around the globe in Marine Corps field bands also possess a significant percentage of college educated professionals in their ranks and demonstrate the dual capability of exercising their advanced skillset while maintaining combat readiness and ability to deploy when called.

Professional military education (PME) is a core value between all elements of Marine music. In addition to perpetual and intense training of individual Marines to grow their specialized capabilities, "The President's Own" provides regular PME throughout the fleet, bringing the highest level of expertise and experience available within the Corps to the occupational field. Musical units in the Marine Corps continually expand the influence each has on the other and share resources to prepare the next generation of Marines to enhance our collective capabilities. Providing significant opportunities for Marines to acquire valuable new skills and leadership responsibility is a critical aspect of operations in the music field. These opportunities are central to both the success of individual Marines and the program in whole, as future leaders must be identified and cultivated from within our unique professional community.

This mentorship philosophy is also regularly shared with the civilian communities each band serves in their commands—as well as across the Nation when musicians travel—through extensive and long-standing educational outreach programs. These significant efforts to reach out to connect with young people not only provide valuable resources and instruction to students at all levels, but it is also a strategic communication tool to encourage the essential support of the communities that are served and a recruiting tool to identify the talent that will become the next generation of Marines.

The very nature of music making and the highly specialized training that is required to perform at an elite level directly aligns with the Commandant's vision to create Marines who "think, decide, and act" and who are "challenged by problems that they tackle as groups in order to learn by doing and from each other." Musicians constantly work to adapt to the evolving mission and learn from each other in realtime each and every day. The success of a musical unit depends entirely on the synergy and chemistry of the team and provides an important and easily understood model for the pursuit of dynamic problem-solving. Further, musical performance is a prime example of the success that is fostered by bringing substantial *individual* talents together to augment the efficacy of the group effort.

Command and Leadership

The high standard of leadership and professionalism in the function of our musical units is on public display for the Marines who see and hear their brothers and sisters perform for them, as well as for the supporting civilian community at large. The occupational field organically empowers Marines to think creatively, grow, and proactively lead as they carry the mantle for so many others who do not have the same public opportunities to represent these qualities on behalf of our Corps.

Music is also critical in reminding all who experience its impact of the innate *human* factor in our Service, both as individuals and as a team. Providing good leadership is dependent on recognizing the inherent value of enriching and nurturing each individual to be at their best. It is remembering that we are indeed at our best as leaders when we take care of our Marines—and each other—physically, mentally, and spiritually. For more than 220 years of shared heritage across so many generations, there has been no more effective way to keep the human aspect of our Service in the forefront of our minds as leaders and comrades-in-arms.

Core Values

Our Commandant reminds us that "the Marine Corps developed its warfighting spirit in the values of honor, courage, and commitment" and that "our rich history demonstrates this ethos and has led generations of Marines to success on and off of the battlefield."

Everything Marine musicians accomplish is designed to embody our core values for the more than 300 million individuals they reach and influence each and every year in person through media and via the ever-expanding digital platforms that have been mastered and leveraged by the occupational field. The commitment and courage Marines display every day in their service is plain to see for those who have opportunity to witness it. It is Marine music that takes on the immense responsibility to tell their story to everyone else both domestically and abroad and to vividly demonstrate what it is that makes Marines different.

In addition to the courage and commitment that is at the foundation of our Corps, it is the concept of honor that is particularly special to Marines, and honor is chief among the sacred values that is best communicated through music. Everything that Marine musicians endeavor to contribute to our heritage is to honor something that is important to our Corps and our country. We honor our fallen with music. We honor our comrades in arms, past and present, with music. We honor our traditions and our identity as Marines with music, and we honor all those who choose to connect with Marines around the world. "The President's Own" Marine Band is further entrusted on the international stage at the White House to honor our very identity as Americans and to represent and honor our artistic and cultural achievements as a country.

In our Service, we are most successful when we are able to bring all of these things together for all people, binding our values as Marines together with our values as a Nation so that they cannot be undone. For nearly as long as we have been an independent Nation and a Marine Corps, music has been at the very heart of that mission.

There is substantial opportunity for leaders in today's Marine Corps to continue to use the power of music to not only amplify the objectives of the *Commandant's Planning Guidance*,[1] but also to strategically engage those who have the greatest influence in perpetuating our Service and setting up every Marine for success. For those leaders who have not had the opportunity to experience that unique power in person, I encourage them to seek out that interaction and take note of the strong and universal emotional impact that can be felt at every single performance given by Marine musicians, whether in ceremony, parades and tattoos, in concerts of all kinds, or in the expansive educational environment. Music is a mode of communication that has been proven time and again to have no equal in our Corps over these past two centuries. It will continue to vividly illuminate our unshakable values and capabilities well into the future.

Note

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

Trident Juncture

Adaptive information and knowledge management

by LtCol Fred Hopewell, USMC(Ret)

The II MEF Information Management Officer's (IMO) mission for TRIDENT JUNCTURE 2018 (TRJE18) was to create an adaptive information and knowledge management (IM/KM) system capable of concurrent support to II MEF, 2D MEB, and 24th MEU command elements, exchanging information and knowledge with multiple commands (Strike Force North Atlantic Treaty Organization [NATO] [SFN], Joint Forces Naples, Norwegians, Canadians) who were afloat, ashore, or back in the continental United States (CONUS) while simultaneously enabling the same at the major subordinate commands and elements (MSC/E) within the task organization.

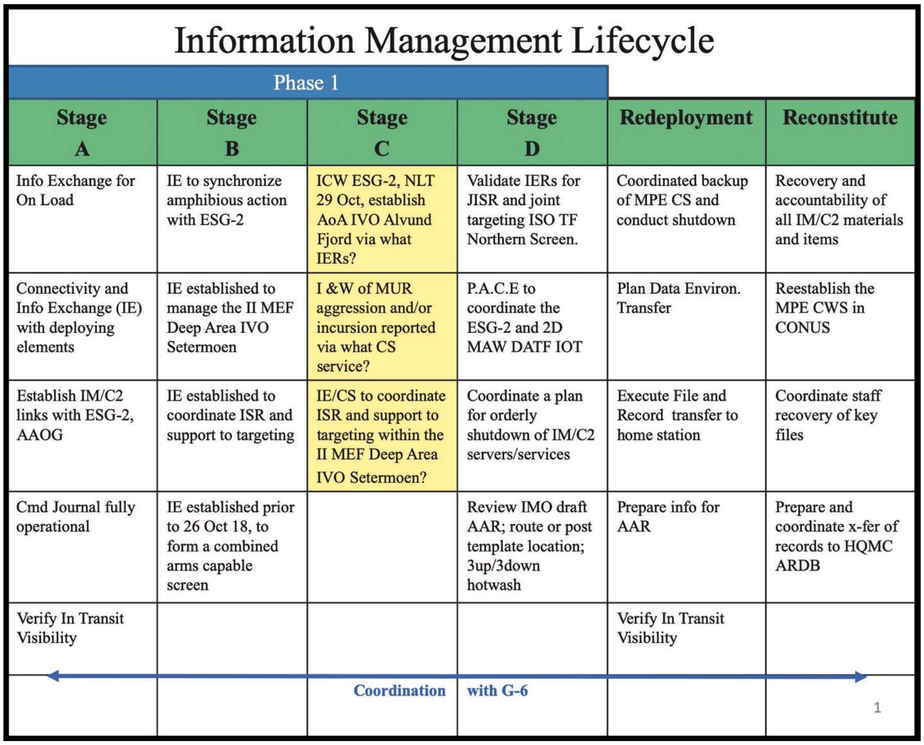
This article will present how the TRJE18 IM/KM mission was accomplished from the perspective of the IMO. It will reveal the IM/KM design theory applied to this NATO exercise, disclose the deliverables aligned to IMO mission essential tasks, summarize what was learned, and provide a recommendation for incorporating this information related capability throughout the Marine Corps.

Design Thinking

Delivering an IM/KM architecture requires trained and certified IMOs applying IM/KM theory to those large organizations; it requires an understanding of the exercise objectives and concept of operations and how users might adapt the digital environment to respond to unfolding events or changes. TRJE18 presented a degree of complexity because of the phasing of MEF and NATO elements, providing knowledge transactions based on existing and widely applied warfighting processes, adapting to changing circumstances, and emergent *ad-hoc* processes while still arranging solutions for knowledge generating, integrating, transferring, and protecting. Additionally, the IMO provides the command more than just sets of tools and technological solutions; the IMO must accomplish the following doctrinal IM/KM mission essential tasks: resolving information processes; establishing and managing the commander's decision-making cycle; engineering systems or applications for both command and functional area use; disseminating shared situational awareness through a common tactical picture; incorporating MEF and MSC staffs' information exchange requirements; and generating the ability for all staffs, internally and externally, to collaborate in a widely distributed and highly mobile environment, amongst a variety of bandwidth sizes. It is quite clear this range of responsibility expands beyond the scope of delivering a single SharePoint site, which is a widely held, Service-wide misunderstanding.

>LtCol Hopewell is the Information Management Officer, II MEF, and temporarily assigned to U.S. Fleet Forces command as the Knowledge Management Officer for Large Scale Exercise 2020.

Equipped with an IM/KM concept of support, the IMO applies a deliberate planning process to develop the IM/KM system. The seven-step planning process works through the solicitation, evaluation, and compilation of collaborative ideas and projects presented by members of the IM/KM Working



Information Management Lifecycle

Phase 1					
Stage A	Stage B	Stage C	Stage D	Redeployment	Reconstitute
Info Exchange for On Load	IE to synchronize amphibious action with ESG-2	ICW ESG-2, NLT 29 Oct, establish AoA IVO Alvund Fjord via what IERs?	Validate IERs for JISR and joint targeting ISO TF Northern Screen.	Coordinated backup of MPE CS and conduct shutdown	Recovery and accountability of all IM/C2 materials and items
Connectivity and Info Exchange (IE) with deploying elements	IE established to manage the II MEF Deep Area IVO Setermoen	I &W of MUR aggression and/or incursion reported via what CS service?	P.A.C.E to coordinate the ESG-2 and 2D MAW DATF IOT	Plan Data Environ. Transfer	Reestablish the MPE CWS in CONUS
Establish IM/C2 links with ESG-2, AAOG	IE established to coordinate ISR and support to targeting	IE/CS to coordinate ISR and support to targeting within the II MEF Deep Area IVO Setermoen?	Coordinate a plan for orderly shutdown of IM/C2 servers/services	Execute File and Record transfer to home station	Coordinate staff recovery of key files
Cmd Journal fully operational	IE established prior to 26 Oct 18, to form a combined arms capable screen		Review IMO draft AAR; route or post template location; 3up/3down hotwash	Prepare info for AAR	Prepare and coordinate x-fer of records to HQMC ARDB
Verify In Transit Visibility				Verify In Transit Visibility	
		Coordination	with G-6		1

Figure 1. TRJE18 information management lifecycle table .

Group (IM/KMWG) and arrives with an executable IM/KM annex.

Deliverables

The result of the IM planning process completes the way in which a MAGTF will collect, manage, filter, fuse, disseminate, protect, and store its information. Based on the challenges of an information architecture spanning from Norway to Iceland to Camp Lejeune, NC, several of the IMO generated deliverables for TRJE18 required innovative approaches and solutions. The first being the way in which information would be managed from deployment to reconstitution, referred to as the information management lifecycle (IML). (See Figure 1 on previous page.)

A lifecycle approach to information and knowledge management during TRJE18 held several advantages:

- It permitted staffs to recognize and effectively focus IM resources in each phase of the exercise lifecycle.
- It anticipated the key information needs of the next phase and prompted staffs to ensure proper coordination occurred in advance.
- It allowed IMOs to manage and monitor information flow through the approved process, using the proper document formats located in the IM matrix, ensuring knowledge sharing takes place by routing products through the appropriate collaborative service or functional area system.

A second TREJ18 output was the "exercise image," which provided the software load for over 30+systems and applications hosted on the mission partner environment. Its use eliminated confusion over specific C2 systems on the client image and aided in troubleshooting through a common sight picture, as referenced in the Annex U. The MEF Chief of Staff, by locking the C2 systems' baseline, contributed to regulating system training requirements, network vulnerabilities and system sprawl, normally produced by connecting unapproved systems or programs.

The third output, the battle rhythm (BR), underwent several iterations to create a balance between decision making and time allocated for leaders and staffs to work, think, and circulate. Properly connecting the MEF BR with SFN BR required eleven modifications before it stabilized. The associated seven-minute drills served as cornerstones to constructing the commander's decision-making cycle, consisting of critical boards, bureaus, cells, and working groups.

The fourth output, collaborative services (CS), a rather new term, provides three methods for the MAGTF to unite across distance through a common workspace, chat, and web conferencing. SharePoint, the collaborative workspace (CWS), leveraged existing MEF policy to establish a simple taxonomy and layout to rapidly access information. *Through the wide use of hyperlinking, adherence to a 2-click rule, and hosting pages vice site collections*, users were able to access BR event spaces and navigate effortlessly through command and staff pages. Relevant text from the CWS could be cut, pasted, and shared with remote units using the chat service, another IMO provided output. JChat was the mission partner environment solution and provided nearly one hundred chatrooms for each MSC, the MEU, MEB, and MEF to conduct warfighting business. Effectively aligning chatrooms to the radio guard chart reduced inquiries and requests for new chatrooms, as chat traffic correlated to radio net functions.

Web conferencing, on the other hand, was not as easily determined as CWS and JChat. Web conferencing was previously accomplished using Adobe Connect Professional. In spring 2017, it was determined by Joint Task Force, Global Network Operations, to possess security vulnerabilities, resulting in the Command, Control, Communications and Computers (C4) Department to rescind its authority to be placed on Marine Corps networks. Secure video teleconferencing (SVTC) offered an alternative solution but is associated with a high bandwidth usage cost, which is not truly conducive to afloat commands but possible through reconfiguration. During TRJE18, SVTC would be limited and restricted to a few terminals. Another consideration, Defense Collaboration Services, hosted by Defense Information Service Agency had proven mission capable stateside, but connectivity to and from Norway was recognized to be ineffective. Fortunately, the MEF IMO, with a long lead time, was able to present this operational gap to MEF and C4 leadership. Left without an enterprise solution for the next twelve to eighteen months, an extensive search arrived at the Marine Corps Enterprise License Management System. Through a series of conversations, it was uncovered Microsoft Skype for Business (SfB) licenses were on the shelf, prompting the IMO to develop the business case and obtain approvals to both acquire SfB and place it on tactical networks.

The basic features of SfB contain instant messaging, voice over IP, and video conferencing inside the client software. Advanced features related to SfB's integration with other Microsoft products include: availability of contacts based on Microsoft Outlook accounts and their retrieval from the Exchange Server, Microsoft Office revealing personnel working on the same document, and communication between clients occurring through a SfB server. This web conferencing solution came together at the start of CPX-2 but was not widely adopted until the execution phase with tremendous success.

The fifth TRJE18 output were performance support systems to address MEF staff issues important to senior leadership. The Executive Decision Support Tool provided executive leadership with a visual display of warfighting function information components, leveraging existing authoritative data sources and reuse of staff products. The Defensive Cyber Event Tracker provided a central location for cyber incident data collection, consolidation, analysis, and reporting. The Data Migration Plan, part of the IML, collected and stored pertinent files and documents, provided for transition of C2 capabilities during the redeployment phase, and directed an orderly deactivation of the MEF's knowledge management architecture.

The sixth TRJE18 output was assembling an experienced IMO team to properly manage and maintain the IM/KM system delivered to the MEF. As TRJE18 confirmed, there is a significant workload to keep the IM/KM system functional and responsive to change as the operation unfolds. For some commanders, it is a paradigm shift to form a team to undertake IM's three mission areas: continuous process improvement, shared situational awareness, and MAGTF collaborative services. These high demand, low density skills are not currently present as part of formal Marine Corps training and are likened to and often assigned as "smart comm guy" tasks; however, this is an overly simplistic view. These are acquired skills best suited for "MAGTF operation types" and take investment in time, money, and experience to acquire. Accordingly, the IMO deployed a twelve-man team, augmented by a remain behind element. While the remain behind element responded to the first mission area, the forward IM team focused on delivering user support to mission areas two and three for the afloat and ashore command elements, with IM leadership present to participate in the BR—simultaneously monitoring and responding to developing events. The deployed team was comprised of three C2 system analyst contractors (CTR), two CS server administrators (CTR), two Command Post Systems Advisors (CTR) for common tactical picture, and C2 systems maintenance. Leadership included the IMO (LtCol), the IM supervisor (GS-14), IM watch officer (USMCR Capt), and MEF IM/C2 liaison officer to SFN (USMCR LtCol). An IM service desk (IMSD) manager (CTR) provided customer interaction and managed 100 TRJE18 service requests (SR) in the first 96 hours, and over two hundred SRs from CPX-1B through the end of the exercise. The IMSD fills a significant role for the IMO due to its continuous process improvement mission and recurring response to changing information needs; therefore, the analysis of IMSD's SRs serve as direct feedback regarding CTR performance, user trends, and system challenges, as well as concurrently aiding the IMO to define, measure, analyze, improve, and control activities within the information environment.

What We Learned

Overall, more was learned about the capabilities and value of IM/KM by the training audience. IM/KM is not entirely focused on technology and sets of tools; instead, it is a 7:2:1 ratio of people to process to technology, which enables the MAGTF to accomplish its mission.

IM/KM activities and initiatives, instead of being additional functions, must be viewed as enabling the commander's decision cycle, ensuring the command is relevant to the speed of the problem.

Equally exceptional takeaways included the following: CS are a critical MAGTF capability; professional and operationalized IMOs are game changers; recognize IM/C2 systems and services can become victims of cyber fratricide.

CS were identified early in the TRJE18 planning process as the IM/C2 center of gravity, which contributed to rapid coordination, decision dissemination, and solution building, spanning from Camp Lejeune to Iceland to Norway. Central to CS for TRJE18 was the value of SfB. During the exercise, SfB use increased considerably with over 620 SfB sessions in the first 96 hours. It delivered exceptional call quality without dropping a single session and an average bandwidth usage of 39Kbps per session—a bandwidth friendly alternative to SVTC. (Note: similar CS software and websites are accessible on Marine Corps NIPRNET and SIPRNET desktops at most duty stations today.)

Another observation was the experience level of the MEF/MSC IMOs: five of the seven had over twelve months in an IM/ KM intensive billet/position. They received extensive formal and on-the-job training through the II MEF Information Management Orientation Course and in various combinations of the Joint Knowledge Management Practitioners' Course, Afloat Knowledge Management Course, Lean Six Sigma Green Belt certification, Information Technology Infrastructure Library Version 3, Project Management Professional, and Information Assurance certifications. Because of the complexity of TRJE18, fourteen IMOs, staff KMOs, and information management analyst contractors completed e-learning and a blended workshop resulting in the industry recognized Certified Knowledge Manager certificate. This experience and professional training enabled them to fully understand how knowledge is formed as well as how their staffs and commands can leverage it. Additionally, the IMOs applied an understanding of how their MSC's performance capabilities and knowledge competencies combine and recombine in new patterns, enabling flexible responses to changing tactical conditions.

A final learning point came following 120-man hours of rebuilding IM/C2 servers and clients over the course of two command post exercises and an MRX. The resolution, coordinated between the IMO and technical control facility located at the communication battalion, was to establish an IMO organizational unit. An organizational unit protects and excludes program of record (POR) systems and applications from receiving cyber updates, which corrupt the POR software. Software corruption in servers and clients required them to be completely rebuilt, which can take up to eight hours per machine. Project and program offices remain solely responsible for coordinating cyber patches and software updates for their PORs. The TRJE18 organizational unit ended service interruptions and equipped the IMO with the correct permissions, to maintain IM/C2 services in an optimal state.

Software corruption in servers and clients required them to be completely rebuilt, which can take up to eight hours per machine.

The Road Ahead

With TRJE18 completed and the after-action report finalized, what can the II MEF IMO suggest institutionally? First is to sustain a continuous IM/KM connection with NATO, U.S. European Command, and United States Naval Forces Europe–Naval Forces Africa. Much can be shared in building a comprehensive approach to this information related capability, honing collective skills through continued participation in exercises such as STEADFAST COBALT, and exchanging tactics, techniques, and procedures through joint/combined IM/KM workshops. Secondly, and more conspicuously, is establishing a Marine Corps IM/KM program. Senior leaders could "focus first on the particular areas experiencing the most unpredictable change"[1] and asking their seasoned IMOs and KMOs how the areas can be stabilized. Restarting a HQMC KM community of interest connecting Deputy Commandants is another promising move; moreover, connecting the Defense Collaboration Services and HQMC departments to Marine Force-level staffs will go a long way in harmonizing and operationalizing command centers at HQMC with persistent combat operation centers at the Marine Forces, MEFs, and their MSCs.

There are many opportunities for cost reductions and cost avoidances by an IM/KM program which will steadily improve overall service performance. The IMO's continuous process improvement capability has already resulted in a business reform initiative and holds further promise in arriving at data-driven programmatic evaluations and informed business decisions. It also can assist in reallocating total obligation authority by eliminating waste and overspending on IM/KM/C2 contractors and redundant capabilities.

A 2017 data call on IM/KM expenditures discovered over $20 million being spent by those organizations whose responses were captured. It is evident an omnibus contract for these services would control and substantiate the required technical skills while spending the appropriate amount for these skills, which is not always achieved by those unfamiliar with the cost of IM/KM/C2 technical service deliverables. Anecdotally, in 2013, $900K was spent on a Microsoft access database worth about $10K.[2] Tactical Radios over Internet Protocol and Wide Area Voice Environment Services also unveiled potential reductions in hardware, maintenance costs, and consumables for providing tactical voice services. There is additional fiscal and organizational value by consolidating the Corps' knowledge in a federated CWS as part of a single information and knowledge enterprise—provided it is properly resourced.

During a 2010 II MEF CPX, the late LtGen Martin R. Berndt, USMC, serving as the senior mentor, questioned the benefit of maintaining two C2 equipment suites: one garrison and one deployed. TRJE18 visibly demonstrated this gap is closing and equipment suites used in garrison are progressing toward a single suite when deployed. Delivering solutions stated in Deliberate Universal Needs Statement (DUNS) 17114DB, Replication and DUNS 17114DA, Marine Corps Enterprise Information Technology Services Support to Tactical Collaboration could close the gap even further—improving access to stateside applications like Automated Performance Evaluation System. In fact, DUNS 17114DB and 17114DA, combined with the POR organizational units, could become part of amphibious ships' architecture, reducing the time it takes Marine commands to install their IM and communications services to less than the current four weeks while facilitating the amphibious readiness group's ability to continue operations, locally, in a communications contested environment. It is important to highlight these DUNS are recommending applying existing technology, which will reduce research, development, testing, and evaluation fiscal outlays. Replication, previously used by 24th MEU during ODYSSEY DAWN and 2d MEB at AGILE LION, is the subject of a December 2019 *Gazette* article, explaining its Service-wide advantage. Regardless, these relatively low-cost DUNS, only ranked 210 and 211 during their fiscal year 2020 review.

Lastly, other no-cost solutions can be incorporated, like having KM programs established in all functional areas and adding IM/KM concepts of support information to all pre- and post-deployment briefs. Notably, another option would be to establish a programmatic requirement across current and future PORs based on the threat. It could require future system budget exhibits to certify interoperability across networks, functions, and applications, and require authenticated application programming interfaces as a deliverable for all PORs and a basis for program funding decisions.

Conclusion

The II MEF IMO delivered the envisioned adaptive IM/KM system for TRJE18 through realization and delivery succeeding mission analysis, collaborative ideas, and projects presented over fourteen months of IM/KMWGs. IM/KM can be focused on the Marine Corps' overall performance and aid high optempo, MAGTF operations, and cross-functionally by optimizing the decision-making cycle and the outputs of functional area processes, rapidly exchanging data, information, and knowledge flagpole to fighting hole. IM/KM performs best when the command IMO is formally trained, remains in the billet two-plus years, and works for the Chief of Staff or XO fulltime. IM/KM is "expensive to do and—if in a highly competitive environment—expensive not to do."[3] Much can be done to make IM/KM prevalent in the Marine Corps, but this will only occur after the Corps decides what it requires from a Service-wide IM/KM program, substantiated by TRJE18.

Notes

[1] Charles Despres and Daniele Chauvel, *Knowledge Horizons: The Present and the Promise of Knowledge Management,* 1st Edition, (Oxford, UK: Butterworth-Heinemann, 2000).

[2] The information is available at https://www.costowl.com.

[3] *Knowledge Horizons.*

More Command, Less Control

Revolutionizing the culture of C2

by Maj Brian Kerg

>Maj Kerg is a Command and Control Officer and a prior enlisted mortarman. He is currently serving as the Fleet Amphibious Communications Officer, U.S. Fleet Forces Command.

A Bloody Lesson

In 2025, a Russian armored division attacked north from Crimea and into the Ukrainian province of Kherson under the false narrative of liberating Kherson's ethnic Russians from Ukrainian oppression. Recalling the consequences of inaction during the Crimean War of 2014, the international community rallied to respond.

Special Purpose MAGTF-Crisis Response-EUCOM deployed as the lead element into the area of operations in order to blunt the Russian advance while surge forces were mobilized. Unfortunately, the Marine Corps failed to change how it exerted command and control (C2) across the battlefield in response to emerging threats in the electromagnetic spectrum (EMS). This set the SPMAGTF up to learn a terribly painful lesson.

Transmissions systems radiated at full power using omni-directional propagation and exercised no emission control, illuminating the unit's approach even before it crossed the line of departure. Predictably, radio checks were made at the top and bottom of the hour, providing Russian electronic warfare (EW) teams with updates on the unit's location and progress. Network on the move, adaptive networking wideband waveform, and other digital interoperability systems that provided an abundance of situational awareness to friendly commanders also broadcast Marine position location information directly into the Russian common operational picture. The battle staff's reliance on unclassified email acted like a sieve, pouring information into the hands of Russian cyber operators. This allowed them to aggregate the information and rebuild the SPMAGTF's plan, thus empowering the Russians to counter every move the Marines made.

At nearly every step toward the objective area, the SPMAGTF was easily detected and targeted with precision. GPS was spoofed and radio nets were jammed; units unused to such tactics struggled to shift to radio nets using spectrum untargeted by electronic attack. As the commander's situational awareness crumbled, he lost tempo, allowing the enemy to outpace him and pound away at the SPMAGTF until it could no longer fight as a cohesive unit. The Marine Corps was forced to "attack in a different direction" once more, retreating from the fight, while the Russian division seized Kherson and reinforced its position.

> **... the MAGTF is not prepared to fight and win tomorrow's wars.**

How We Got Here

The *38th Commandant's Planning Guidance* (CPG), on its first page, concurs with the assessment of the *Marine Corps Operating Concept* (MOC) that the MAGTF is not prepared to fight and win tomorrow's wars.[1] The CPG outlines several critical initiatives that the Service must pursue to alleviate this problem, and there is a lot of goodness happening in many corners of the Corps to see the CPG's vision realized. But it is not enough, with the most grievous shortcoming residing within how we conduct C2. Though our most senior leadership has issued the clarion call for change, we still are not there. Why not?

Quite simply, the culture of C2 does not adequately account for the enemy and prioritizes control over command, hampering our ability to complete one of the CPG's goals: exert C2 in a degraded environment.[2] Commanders and staffs have grown up in a C2 culture where they enjoyed a plethora of C2 systems that gave them incredible situational awareness and control over subordinate units while fighting an adversary with no EW capability. With greater access to more information, we have demanded more frequent and elaborate reporting, placing tighter and tighter control over our subordinate units. We have come to expect ubiquitous access to connectivity and data services that replicate what we enjoy in the civilian world, to the extent that a video teleconference is a baseline standard by which to communicate even among major subordinate elements. We have gone so far as to adopt industry standards of information technology certification for our Marines.

The problem with all of this is that the industry and the civilian world do not have to account for the enemy. We as a Service have been able to get away with these excesses because we have grown used to fighting non-state actors without the capability to punish us for being lazy in the EMS. This has created bad habits and systemic obstacles to the application of our maneuver warfare philosophy. Rather than building fluid C2 structures that are informed by the operational environment that can dynamically shift systems based off of enemy capabilities, we erroneously recreate cumbersome, vulnerable, identical C2 architectures for every operation and exercise—regardless of the enemy threat.

Without a radical reappraisal of how we as a Service enable and practice C2, we will be setting ourselves up for a costly failure similar to that described in the opening vignette. We will fail to accomplish our mission and see our Marines pay an unnecessary cost in blood. We can embrace change now, using information we already have, or be forced to change later—after we pay the butcher's bill.

Effective C2 faces several challenges. ***(Photo by PFC Ulises Salgado.)***

Bad C2 Habits, Good C2 Doctrine

Talk to the evaluators of integration training exercises. Reach out to those who have participated in force-on-force free-play exercises. Talk to experienced and honest S-2, S-3, and S-6 officers and chiefs in a non-disclosure environment. Though much of the self-reporting that we as a Corps make public is self-congratulatory and consistently positive, those on the ground will tell you a different story. The C2 problem is both real and endemic.

The luxury of an uncontested EMS and unimpeded situational awareness has created a number of challenges. We fail to apply signature management, thus giving away our positions and intentions by how indiscriminately we employ transmissions systems. Many commanders and staffs are visibly uncomfortable exercising C2 over radio nets. When denied the ability to use email, we grow frustrated and claim that we cannot send required reports. When bandwidth limitations restrain us from sending massive power-point files, we fail to convey the information in a meaningful way. Because our previous adversaries did not try to contest the EMS, we expected that the S-6 would always be able to "lay the pipes" to support any concept of operations (CONOPS) and make the plan work, so we never invited him into the room during problem framing or challenged him to plan for a contested environment if we did.

The irony is that we already have the answer to this dilemma. Principles for effective C2, despite the rapid technological changes that have seemingly revolutionized the way future wars will be fought, exist in *MCDP 6, Command and Control*.

How do we define effective C2? "Since war is a conflict between opposing wills, we can measure the effectiveness of C2 only in relation to the enemy."[3] Effective C2 is not necessarily email and the video teleconference—though it could be if the situation warrants it. Effective C2 is whatever enables us to beat the enemy. If semaphore and Morse code allow us to perform at a greater tempo than the enemy and destroy his cohesion, then we have succeeded.

The expectation of constant access to full spectrum C2, inclusive of all forms of video, voice, and data, naturally creates a greater appetite for more information, even when it cannot meaningfully contribute to our decision-making process.[4] When commanders can get more, they ask for more, even when the bias for more information puts them at risk of information paralysis.[5] *MCDP 6* warns against this: "We should accept that the proper object of C2 is not to be thoroughly and precisely in control. The turbulence of modern war suggests a need for a looser form of influence."[6] This warning becomes even more prescient when we recall that the most current edition of *MCDP 6* was written in 1996. The problem described remains the same, despite the exponential changes that have occurred in C2 systems in the last 24 years. So how do we overcome these obstacles?

Creating Effective C2

Again, *MCDP 6* tells us what concepts must be applied to achieve effective C2, despite the technologies involved. Mission type orders, low-level initiative, commander's intent, mutual trust, implicit understanding, and other fundamentals of our maneuver warfare philosophy are prerequisites for effective C2.[7] But if it were that easy, we would be there already, and the defeat described in the opening scenario could never play out. What follows, then, are critical cultural changes that must occur within our organization if we hope to avoid such an outcome. It is nothing short of cultural because we are not thinking of or practicing C2 as it is described in our doctrine because we, as a Service, have not needed or wanted to.

Information trumps the medium, and sometimes less is more. Do you really need a video teleconference to conduct a meeting, or would a conference call work instead? Is a 50-slide PowerPoint presentation with high fidelity pictures needed for your daily submission for the commander's update brief, or can you convey the same information with bullet points sent via text over a radio? If you just communicated with a subordinate unit on the radio, must you still conduct a radio check in ten minutes because it will be the top of the hour, or have you just validated that the net is up? Do you really need to emit signal with constant checkpoint updates on the net as you move to the assault position, or can you wait to give away your position in the spectrum until you need to coordinate fires on the objective and must give up your position anyway?

The situation will dictate, but ultimately the need to get information to the right people trumps the medium over which you pass that information. Commanders should set this expectation at every level, staff members should get comfortable operating this way, and C2 planners should employ the most reliable system appropriate to the threat, rather than always defaulting to building the most complex and fragile C2 structure they can.

Embrace the contested electromagnetic spectrum and make threat informed C2 plans. Our adversaries can contest the EMS, and many of their capabilities are public knowledge. For example, the table of organization for the Radio Electronic Battery, which is organic to the Russian brigade, describes systems that are layered to contest SATCOM, GPS, cellular, and other signals at the tactical level.[8] Their threat ranges are known and can be planned for now. In some instances, how we have grown up employing C2 systems is akin to a rifleman on a night patrol lighting a cigarette. In other cases, it is like setting a bonfire in the dark. In both cases, we present a target indicator and invite the enemy to shoot us.

Planning for this reality should be SOP for every unit at the battalion level and higher. The S-6 and S-2 should develop a modified combined obstacle overlay (MCOO) that incorporates C2 in a C2-modified combined obstacle overlay (C-MCOO) that informs the commander when and where the adversary can detect or target his C2 systems. The S-2, S-3, and S-6 should develop C2 plans that allow the battle staff to shift fires from one C2 system to another depending on what is being contested and what threat is being presented. Commanders should set the expectation that their staffs can continue to operate in a contested environment, using less than ideal mediums for information exchange. Primary, alternate, contingency, and emergency (PACE) plans must account for all information exchange requirements, and not just for the video, voice, and data (i.e., the Advanced Field Artillery Tactical Data System). C2 planners must become as familiar with enemy EW systems as they are with their own C2 systems and also make clear, meaningful recommendations on a C2 architecture that accounts for the environment and the threat.

... C2 planners should employ the most reliable system appropriate to the threat, rather than always defaulting to building the most complex and fragile C2 structure they can.

Operate a PACE plan, even in garrison. PACE plans are briefed and practiced in a tactical environment, but they are difficult to execute smoothly because staffs are not used to executing them. Not only because the EMS was not contested in Iraq and Afghanistan, but also because we only think about a PACE plan when we are in an exercise or operational environment. When we are in garrison and the network goes down, it is not uncommon for those with information exchange requirements to pack up, go home, and continue working over commercial Internet.

Commands, at the battalion level and higher, should have a PACE plan for their garrison network, and it should be published and executed as the norm. You might not be able to send your product on an email, but you can burn it to disk, hand it off to someone with a vehicle, and run it to the command post. Personally traveling to your subordinate leaders for a face to face conversation is a very powerful form of the C2 cycle because you get immediate feedback—the "control" in the C2 feedback loop—based off the subordinate's reaction to your commands. Perhaps going home and using commercial Internet *is* part of the PACE plan—but this should be a deliberate, planned choice, and not something that occurs incidentally. Commanders should demand that a garrison PACE plan be used as SOP. C2 planners should build meaningful PACE plans that cover every form of alternate garrison C2 system, inclusive of DSN phones, burning files to disk, messengers, personal conveyance, and anything else that gets the job done.

Employ the S-6 as a C2 officer, not a communications officer. What's in a name? An awful lot, and it shapes how commanders and staffs employ the S-6. As a communications officer, the S-6 is not tied directly to a warfighting function. Compounded by the fact that the table of organization has the S-6 as one of the most junior members on any staff, he is rarely seen as anything more than a network pipe-layer who builds architecture to the specifications of the CONOPS. However, this robs the commander of a subject matter expert who can help shape the CONOPS, especially in EMS contested environments. That same S-6 should also know the signature that his systems emit, the ability of adversaries to detect friendly forces based on how those systems propagate their signals, and how to advise the commander to use C2 systems to minimize detection, targeting, and destruction.

Redesignate the 0602 from a "Communications Officer" to a "C2 Officer,"

Train our Marines to account for C2 in a contested environment. ***(Photo by Sgt Conner Robbins.)***

and plug that staff officer into the warfighting function of C2. Demand that your S-6 master the EW threat to the C2 capabilities he provides the commander. Expect the S-6 to team with the S-2 to become an expert in adversary EW. Direct the S-6 to work with the S-3 to make C2 plans that account for adversary threats, even (and especially) if those plans have significant impact on the concept of operations, because they can and they will. Turn the S-6 into a C2 tactician and enable him to rise to that task with how he is employed. Make the sacrifice in time to send your S-6 to the MAGTF Communications Planners Course where he will learn to be the C2 tactician he needs to be to succeed in the future fight.

Start the change at the entry level and maintain it at follow-on training. Learning to adjust the C2 method to the environment and the threat cannot wait until after leaders have spent over a decade learning bad habits; changing your fundamental outlook on warfighting when you are closer to retirement than not is a tall order. It is as unfair as it is unrealistic, but ultimately it is dangerous. This training must begin at the entry level and be sustained throughout the career-long training continuum.[9]

Lieutenants need to be taught at The Basic School how to account for C2 in a contested environment and how it will affect how they can expect to employ C2 systems. Infantrymen need to learn this at the School of Infantry, and Transmissions Systems Operators need to train to these tactics at Marine Corps Communications Electronics School. Incorporate planning and supervision tasks for this threat at follow-on schools, including Small Unit Leader's Course, Transmissions Chief's Course, and Expeditionary Warfare School. Critically, incorporate C2 planning against pacing threat EW capabilities into the curricula offered by the Marine Corps Tactics and Operations Group as this will provide training to future CGE operations officers and chiefs.

> ***For too long, we as a warfighting organization have become sloppy in how we practice C2.***

Revolutionize the C2 Culture

For too long, we as a warfighting organization have become sloppy in how we practice C2. Decades of war against adversaries with no capability to contest the EMS, combined with increasingly complex C2 systems that offer bountiful situational awareness, have turned us into gluttons for information. The demand for greater control is a detriment to effective command. This prevents us from realizing the vision of the CPG and impedes our ability to win a conflict against our pacing threat.

By applying the fundamentals of our C2 doctrine to the current threat, we can turn this ship around. The methods to do this are varied, but they ultimately require a radical change in the culture of how we conduct C2 across the Marine Corps. Leaders at every level must embrace this change today, so we can win the fight tomorrow.

Notes

[1] Headquarters, Marine Corps, *38th Commandant's Planning Guidance*, (Washington, DC: 2019).

[2] Ibid.

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

[4] Jonathan Baron, *Thinking and Deciding, 2nd edition,* (Cambridge, UK: Cambridge University Press, 1994).

[5] Lon Roberts, *"Analysis Paralysis: A Case of Terminological Inexactitude," Defense AT&L*, (Fort Belvoir, VA: Defense Acquisition University, January-February 2010).

[6] Ibid.

[7] *MCDP 6, Command and Control.*

[8] Asymmetric Warfare Group, *Russian New Generation Warfare Version 2.1*, (Fort Meade, MD: Asymmetric Warfare Group, 2016).

[9] Christopher Paul, et al., *Situational Awareness for Operations in and Through the Information Environment*, (Santo Monica, CA: RAND Corporation, 2018).

Maneuver Warfare in the Cyber Domain

A proposal to update the existing legal framework to facilitate decentralized decision making in cyber operations

by Capt Joe McGinley

> *War is both timeless and ever changing. While the basic nature of war is constant and methods we use evolve constantly … [o]ne major catalyst of change is the advancement of technology. As the hardware of war improves through technological development, so must the tactical, operational, and strategic usage adapt to its improved capabilities to counteract our enemy's.*[1]

This excerpt from *MCDP 1, Warfighting,* has proven particularly relevant with the advent of cyber warfare. Recent technological advances have allowed hackers to conduct cyberattacks against the United States and countries around the world. The 2015 Office of Personnel Management hack, for example, resulted in the theft of 21.5 million Federal employees' personal information. In 2007, a series of coordinated cyberattacks crippled the Estonian government, banks, media, and other institutions—bringing the country "to a virtual standstill."[2] Most recently, Russia has employed cyber operations as part of the conflict in Ukraine.[3]

>Capt McGinley is currently the Deputy Staff Judge Advocate at Marine Corps Base Hawaii. Prior to MCBH, he was a trial counsel at MCAGCC Twentynine Palms, CA and deployed with the Marine Rotational Force-Darwin.

In the absence of treaties or statutes, the DOD and Marine Corps have taken steps to adapt to and regulate this new wrinkle in modern warfare. Several DOD documents relevant to this discussion are classified; those documents will not be addressed and limit this article's permissible scope.

The United States does not stand alone in its quest to regulate cyberspace and cyber warfare. An international group of experts developed the *Tallin Manual* and *Tallin Manual 2.0*, which seek to establish an international code to govern cyber operations. While the *Tallin Manual* and the *Tallin Manual 2.0* provide useful guidelines, they are not binding on the United States. It would benefit the United States to take a leading role in the development of domestic and international standards, both as a world leader and because such standards will improve America's ability to act and react decisively, consistently, and in coordination with our allies.

Current Legal Framework

Modern warfare is analyzed under two primary sources of authority: the U.N. Charter and the Law of Armed Conflict (LOAC). Cyber warfare, however, presents several challenges that the definitions in the U.N. Charter and the LOAC may not adequately address.

The U.N. Charter. The U.N. Charter establishes many of the basic principles for international relations. Various interpretations of the U.N. Charter have occasionally resulted in political tensions, such as balancing a state's right to sovereignty with a state's right to preemptive self-defense. Sovereignty versus preemptive self-defense remains an ongoing source of friction in international relations and international law—a problem that will be exacerbated if the conduct of cyber warfare is analyzed within a framework that does not account for its intricacies.

Article 2 of the U.N. Charter grants states the right sovereignty, stating,

> [a]ll Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.[4]

Article 51 grants states the right to self-defense. It reads, in part,

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an *armed attack* occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security [emphasis added].[5]

The U.N. Charter, understandably, does not address issues specific to cyber warfare in several ways. The U.N. Charter does not define the "force" that may not be used "against the territory integrity" of any state, nor does it define "armed attack." Cyberattacks resulting in physical damage, and thus having the effect of a physical attack, would likely constitute force in violation of Article 2. One could argue, however, that cyberattacks that *do not* result in the manipulation of physical objects (such taking information from an electronic database) may not constitute "force" against a state's "territorial integrity" as the terms are commonly understood. This represents a potentially dangerous gray area, and one that our enemies could exploit.

Additionally, as with traditional warfare, no clear guidance exists on how far the right to self-defense, as articulated by Article 51, extends. A state's right to self-defense is not absolute, and it remains unclear when action in cyberspace crosses the line between "preemptive self-defense"[6] and a violation of another state's sovereignty.[7]

The LOAC. The DOD applies the LOAC to all military operations. The LOAC is a combination of the "Hague Tradition" and "Geneva Tradition."[8] The Hague Tradition regulates the means and methods of warfare, such as the tactics, weapons, and targeting criteria.[9] All military operations must be evaluated in terms of necessity, proportionality, distinction, and humanity.[10]

The LOAC applies to both international armed conflicts (IACs) as well as non-international armed conflicts (NIACs). However, the distinction between the two categories of conflict could prove critical to other issues such as use of force and the status of enemy combatants. The ability to attribute an attack to its source will be crucial in determining whether an IAC or NIAC framework applies.

IACs. The U.N. classifies armed conflict between two states as IACs. It bases this classification on Common Article 2,[11] which is supplemented by Additional Protocol I.[12] Cyber warfare in an IAC poses few legal problems. If a foreign military or government conducts cyberattacks against the United States as part of a conflict, the United States could respond in accordance with U.N. Charter Article 51 and the LOAC, constrained only by the principles of necessity, distinction, proportionality, and humanity. Those foreign operatives working on behalf of the state would be entitled to the same protections as any other prisoner of war.

NIACs. The more complex scenario would involve one or more non-state actors that conduct cyberattacks against the United States. One can easily imagine a scenario in which a terrorist organization, or other organizations operating independently of any nation-state, attempts to bring down all or parts of the DOD or Marine Corps network. These actions and actors would likely fall within the NIAC framework.

NIACs, or "armed conflict[s] not of an international character occurring in the territory of one of the High Contracting Parties,"[13] trigger additional Protocol II obligations for the state party involved in the conflict.[14] NIACs have traditionally involved the imposition of international regulations on entirely internal conflicts, such as the Colombian government's struggle against the Revolutionary Armed Forces of Colombia. But this definition has expanded in recent years; multiple international courts have recognized that NIACs may exist across international borders.[15]

Unlike combatants in IACs, combatants in NIACs do not receive combatant immunity, prisoner of war status, or protections for their actions.[16] Foreign cyber operatives will likely fall somewhere along a spectrum between "no state support" and "state or military employee." The Marine Corps should have a plan for how to classify actors at various points along this spectrum, providing various levels of support, and train Marines on what protection those actors are entitled to. Once we accurately categorize these actors, we will next have to determine at what point they become valid military targets depending on their actions in cyberspace. Commander's intent should then empower decision-makers at the appropriate level.

How far does our right to self-defense go? **(Photo by LCpl Angela Wilcox.)**

Improving our Combined Arms

The Marine Corps relies on maneuver warfare to defeat its enemies. Part of this approach includes the use of combined arms, which *MCDP 1* defines as "the full integration of arms in such a way that to counteract one, the enemy must become more vulnerable to another."[17] Speed provides a crucial means to exploit the enemy's gaps that the combined arms dilemma exposes. The cyber domain is no different.

The Marine Corps is aware that its reliance on electronics could prove to be a critical vulnerability in battle. A successful enemy cyberattack could act as a force multiplier for an otherwise inferior force, drastically slow our operational tempo such that we lose relative speed over the enemy, and severely limit the Marine Corps' ability to use combined arms. In a near-peer engagement, the ability to move our personnel and aircraft close to and into enemy territory both undetected and unimpeded will be critical for shaping operations. Developing cyber capabilities organic to the MEFs and empowering decision-makers at the MEF level would allow for a quicker response, thus improving our relative speed and exposing our enemies to a combined arms dilemma earlier in the fight.

Moving Forward

Domestically, the United States has recognized the immediacy of the cyber threat, as evidenced by the 2017 *National Security Strategy* and the 2018 *National Defense Strategy* (NDS). While discussing how to protect the United States in the cyber era, the *National Security Strategy* noted that information sharing and layered defenses will be key to deterring and defeating rogue actors.[18] The NDS enacted this intent, stating that we will

> invest in cyber defense, resilience, and continued integration of cyber operations into the full spectrum of military operations.[19]

The Marine Corps Cyberspace Command addresses and develops defenses to cyberattacks, assesses system vulnerabilities, and prepares to digitally "maneuver" in support of operational forces.[20]

Internationally, the *Tallinn Manual* distinguishes between "use of force" and "armed attack"[21] and concludes that cyber operations can qualify as an armed attack, particularly in cases involving substantial injury or physical damage.[22] Additionally, some members of the group posited that a "sufficiently severe non-injurious or destructive cyber operation, such as that resulting in a state's economic collapse, can qualify as an armed attack."[23]

These domestic and international measures represent a great deal of progress and a useful baseline in an emerging field. The United States should seek to lead the global community in this area. The DOD will benefit from having a set of rules for responses and engagement criteria. While not a necessity, signing and ratifying a single international framework can both improve relations with our allies and allow the DOD to improve interoperability during combined operations. Such a framework will also facilitate decentralized decision-making as to whether an "attack" has occurred and allow MEFs to respond quickly and decisively in fluid situations.

Decentralized decision-making remains especially important to the Marine Corps. Our structure and doctrine place decision-making responsibility on our personnel closest to the ground. Predictability and known rules of engagement may become critical considerations for these individuals. Our MAGTFs and MEFs would benefit from an organic cyber warfare element

We rely on maneuver warfare to out think our enemies. *(Photo by Cpl Mark Lowe.)*

The personnel closest to the ground are the responsible decision makers. *(Photo by Cpl Mark Lowe.)*

that could react instantaneously to an enemy cyberattack, conduct a counterattack, and relay relevant information to the GCE, ACE, or LCE. Such decentralization is also consistent with the NDS's directive to integrate operations "into the full spectrum of military operations." Cyber and electronic warfare will likely take on an increasingly prominent role in future conflicts; we owe our Marines the power to make critical decisions with confidence and consistency so we may continue to win battles in any clime and place.

Notes

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

[2] LTC Scott W. Beidleman, USA, *Defining and Deterring Cyber War*, (Carlisle, PA: U.S. Army War College, 2009).

[3] Laurens Cerulus, "How Ukraine Became a Test Bed for Cyperweaponry," *POLITICO*, (February 2019), available at https://www.politico.

[4] United Nations, *Charter of the United Nations,* (San Fransico, CA: October 1945). See Article 2 (4).

[5] *Charter of the United Nations*. See Article 51.

[6] U.N. Special Rapporteur Philip Alston has stated that

> [a] targeted killing conducted by one State in the territory of a second State does not violate the second State's sovereignty [where] ... the first, targeting State has a right to international law to use the force in self-defen[s]e under Article 51 of the U.N. Charter, [and] the second state is unwilling or unable to stop armed attacks against the first State launched from its territory.

U.N. Human Rights Council, *Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Study on Targeted Killings, U.N. Document A/HRC/14/24/Add.6*, (Geneva, CH: May 2010). For other examples of preemptive self-defense in international law, see William H. Taft IV, *The Legal Basis for Preemption*, Council on Foreign Relations, (2002), available at http://www.cfr.org

[7] In traditional warfare, absent consent, a "victim" state may only violate another state's sovereignty in the name of self-defense if the host state is "unwilling or unable" to stop the threat to international peace. Additionally, the victim State's operations must conform to the LOAC's principles of necessity and proportionality. A similar standard would be useful cyber warfare, especially considering the clandestine and secretive nature of some hacking groups in countries like China and Russia. See Ashley S. Deeks, "'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense," *Virginia Journal of International Law*, (Charlottesville, VA: University of Virginia School of Law, December 2011). Citing Permanent Rep. of the Russian Federation to the U.N., Letter dated Sept 11, 2002 from the Permanent Rep of the Russian Federation to the United Nations addressed to the Secretary-General, Annex, U.N. Doc. S/2002/1012/Annex.

[8] LTC Richard P. DiMeglio, Judge Advocate, USA, et al., *Law of Armed Conflict Deskbook*, (Charlottesville, VA: United States Army Judge Advocate General's Legal Center and School, 2012).

[9] Hague tradition consists of the Hague Conventions of 1899, as revised in 1907, the 1954 Hague Cultural Property Convention, and the 1980 Certain Conventional Weapons Convention. Geneva Tradition focuses on respecting and protecting victims of warfare; Geneva Tradition is composed of the four Geneva Conventions of 1949, each of which protects a different category of war victim. *Law of Armed Conflict Deskbook*: *supra* n. 8 at 19.

[10] *Law of Armed Conflict Deskbook.*

[11] "Common Article" refers to articles that are common to all four Geneva Conventions.

[12] "[T]he present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more High Contracting Parties, even if the state of war is not recognized by one of them." Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field ["Geneva I"] article 2 (1949). The United States has not signed or ratified Protocol I, in part because it expands Common Article 2 to include conflicts previously classified as non-international armed conflicts. Under Protocol I, Common Article 2 would include "armed conflicts in which people are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination." Protocol Additional to Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts art. 1, para. 4. The United States has resisted ratifying Protocol I because it expands liability for commanding officers for the actions of subordinates (*id.*, at arts. 86, 87) and because it states enemy combatants have not distinguished themselves from civilians until they have engaged in preparatory or combat activities (*id.*, at art. 44[3]). For a fuller discussion of the reasons that some States have chosen not to ratify Protocol I; see Harvey Rishikof, "Institutional Ethics: Drawing Lines for Militant Democracies," *Joint Force Quarterly,* (Washington, DC: National Defense University Press, 2009). See also David McGrogan, "Whither Now, Additional Protocol I?" *International Law Observer,* (January 2009), available at http://www.internationallawobserver.eu.

[13] *Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field ["Geneva I"] art. 3 (1949).*

[14] *Law of Armed Conflict Deskbook.*

[15] See Supreme Court of the United States, *Hamdan v. Rumsfeld, 548 U.S. 557,* (Washington, DC: 2006). Holding that "the term 'conflict not of an international character' is used here in contradistinction to a conflict between nations" and thus recognizing that Common Article 3 conflicts can expand beyond the territory of one States. See also International Court of Justice, 2005 I.C.J. 337, *Case Concerning Armed Activities on the Territory of Congo (Democratic. Republic of Congo v. Uganda),* (The Hague, NL: December 2019).

[16] For further reading, see Supreme Court of Israel, *HJC 769/02, The Public Committee Against Torture in Israel, et al., v. The Government of Israel, et al.*, (Jerusalem, IL: December 2005).

[17] *MCDP 1.*

[18] *National Security Strategy of the United States of America, 2017.*

[19] *National Defense Strategy of the United States of America, 2018.*

[20] James K. Sanborn, "Cyber Battlefield Grows in Importance," *Military Times,* (April 2009), available at http://www.militarytimes.com.

[21] Collin Allan, "Was the Cyber Attack on a Dam in New York an Armed Attack?" *Just Security,* (January 2016) available at https://www.justsecurity.org.

[22] Ibid.

[23] Ibid.

Transforming Marine Corps Operations in the Information Environment Training

Gaining and maintaining an operational advantage

by LtCol James McGrath, LTC Tim J. Pike, USA(Ret),
CDR Christopher Pieczynski, USN(Ret) & Capt Michael Runyon

>LtCol McGrath is a Cyberspace Operations Officer currently serving as the Operations Officer for III Marine Expeditionary Force Information Group.

>>LTC Pike is a former U.S. Army Information Operations Officer and is currently the Lead IO Curriculum Developer and a Senior Instructor at Expeditionary Warfare Training Group, Atlantic.

>>>CDR Pieczynski is a former U.S. Navy Surface Warfare Officer and is currently an IO Curriculum Developer and Instructor at Expeditionary Warfare Training Group, Atlantic.

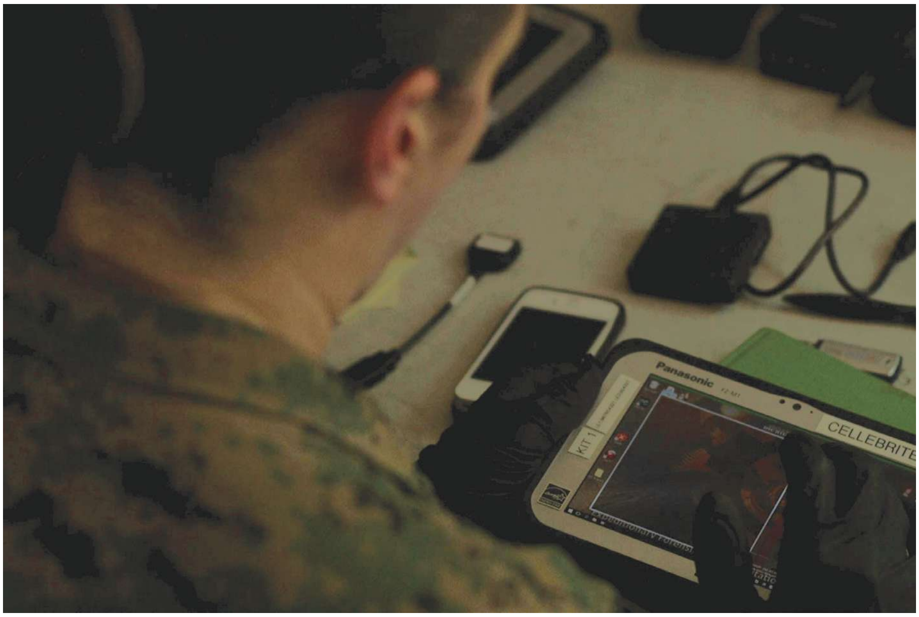
>>>>Capt Runyon is a Counterintelligence/Human Source Intelligence Officer currently serving as an Intelligence Officer aboard Naval Station Guantanamo Bay.

More than ever the Marine Corps is faced with the challenge to "secure or protect national policy objectives by military force when peaceful means alone cannot."[1] The rapid proliferation of information technologies has made this more difficult. The Fleet Marine Forces (FMF) have already begun to implement structure changes to support this, but current operations in the information environment (OIE) training must be revised in order to train the next generation of creative, adaptive, and disruptive OIE leaders with the knowledge and skills to intuitively fight and win in today's complex, information-dependent operating environment. Expeditionary Warfare Training Group, Atlantic is already postured to provide this training once changes are made to current MOS models and training and readiness functional areas.

Military Problem

The rapidly changing operating environment faced by today's Marine Corps consists of a landscape where our adversaries have access to precision weapons; advanced intelligence, surveillance, and reconnaissance capabilities; stealth technologies; and sophisticated command and control (C2) capabilities.[2] Even more alarming is that these adversaries are demonstrating advanced forms of information warfare that can threaten the assured C2 of our forces, deceive our commanders and intelligence systems, and ultimately psychologically undermine the morale of our Marines and attack the will of our allies and coalition partners.[3] The overall objective of Marine OIE is not just to meet the enemy on the 21st century battlefield but to develop and operationalize a capability to gain and maintain operational advantage over the adversary on that battlefield or simply put, to man, train, and equip our Marines to achieve that advantage. To achieve this ambitious goal, a foundation of individual knowledge, skills, and abilities must be instilled into a cadre of OIE officers and enlisted men and women who can readily understand and maneuver within today's dynamic and highly contested information environment.[4]

In order to effectively control OIE capabilities, resources, and activities, the Marine Corps must cultivate an advanced cadre of individuals who are skilled in the integration, synchronization, and coordination of all functions of the OIE and their supporting capabilities, which is currently achieved by OIE officers and enlisted specialists. Currently, the Marine Corps has two resident courses at Expeditionary Warfare Training Group, Atlantic to train OIE practitioners:



The Marine Corps must develop a cadre of Marines who are readily able to operate within the information environment. *(Photo by Sgt Luisa Torres.)*

- Two-week Intermediate MAGTF Information Operations (IO) Practitioner's Course (IMIOPC), leading to the Basic IO Staff Officer, 0510, and the IO Specialist, 0551, MOSs
- Three-week Advanced MAGTF IO Planner Course (AMIOPC), leading to the Advanced IO Planner, 0550, MOS. It should also be noted that IMIOPC is one of two requirements for achieving the Psychological Operations (PSYOP) MOSs, PSYOP Officer, 0520, and PSYOP NCO, 0521.

This current training construct used by the Marine Corps was well designed to meet the needs of the fleet as the Marine Corps first began to develop its ability to fight in the modern information environment. However, as our understanding of the information environment continues to develop and mature, our ideas and methods for training OIE Marines must also evolve so that the next generation of Marines can effectively advise, plan, execute, and assess OIE across the full range of information functions and capabilities.

At present time, the Marine Corps' OIE training continuum effectively develops information planners designed to integrate information capabilities into the Marine Corps Planning Process and is focused almost exclusively at the tactical level. However, as the past 19 years of conflict in Iraq and Afghanistan has revealed, creating tactical planners is not enough for the Marine Corps to dominate the 21st century information space. Simply put, there are other critical skills required to gain and maintain an advantage that are not currently taught within the IMIOPC and AMIOPC curricula. These critical skills are gaps in our current training model. Correcting these gaps will provide Marine OIE planners with the additional knowledge, skills, and abilities to effectively advise the commander regarding all information environment activities, manage execution, and implement a well-integrated assessment plan at both the tactical and operational levels of war.

> ***... creating tactical planners is not enough for the Marine Corps to dominate the 21st century information space.***

Also, in order to discuss improvements to the OIE training continuum, we must first understand our own obstacles in the development of a core group of well-trained, experienced OIE practitioners available to the FMF. The most glaring obstacle is the current Marine Corps OIE planner MOS model. The current model draws practitioners from the Marine Corps without any consideration of a Marine's prior knowledge and experience with OIE. For instance, a Marine may serve one tour in an OIE billet and then never work in this critical field again. Or worse, because the OIE MOSs are free MOSs (FMOS), a Marine may serve in multiple OIE billets and ultimately hurt their chances for promotion because they have spent too much time out of their primary MOS (PMOS) and no longer have the requisite experience within their PMOS for favorable consideration. Recognizing these challenges and the fact that the Marine Corps will not have a permanent, professionalized cadre of PMOS trained OIE practitioners[5] in the foreseeable future, only heightens the importance of ensuring that both IMIOPC and AMIOPC are well designed, implemented, and executed.

OIE Training Solution

Keeping these challenges in mind, there is a need to expand OIE training beyond the previous single training and readiness (T&R) manual planning function into three additional functional areas. The full complement of required T&R manual functions includes advising, planning, execution, and the assessment of information plans and activities. Expansion beyond planning allows the OIE students to leave the training environment with the knowledge of "how to" do their job throughout the entire spectrum of operations and the seven broader functions of OIE. The remainder of this innovation initiative focuses on fully outlining these four T&R functional areas and providing recommendations for the way forward.

The first OIE T&R manual functional area is advising. Advising is done continually throughout all types and phases of operations and is critical to the command in all phases of planning, execution, and assessment as the commander works through operational design, provides planning guidance, commander's intent, and continues to make decisions. As the leader of the integration, coordination, and synchronization of all information capabilities, the senior OIE officer, FMOS 0550 or 0510, is the single best person to advise not only the commander but the rest of the staff on the effects of information capabilities in the information environment and how those effects can best lead to an operational advantage. Some areas the OIE practitioner should be able to advise the commander on are current technologies and tactics associated with the command's array of organic and nonorganic information capabilities; the seven functions of information; the six OIE capability areas; adversary and allied information warfare doctrine; information capability policy, law, and associated authorities, specifically military deception (MILDEC), PSYOP, electronic warfare, cyber, operations security (OPSEC), space operations, and special technical operations; emerging trends, such as the convergence of space, cyber, and electromagnetic spectrum domains; hybrid and nonlinear warfare; near peer and pacing threats; and the latest techniques for naval and joint OIE integration.

The second T&R manual functional area, which Marine Corps OIE already does fairly well, is planning. Planning has historically been the focus of OIE training and is currently the strength of OIE training both in the Marine Corps and in the joint community. Improvements that can be made in this area are increased information environment analysis by introducing topics such as social network analysis, narrative development, and the application of behavior and communication theories, both technical and cross-cultural. The expansion of the planning function in the advanced course should include operational design with a systems-thinking approach and an introduction to the joint operations planning process. Lastly, the joint MILDEC and OPSEC planning processes coupled with signature management (SIGMAN) should be enhanced for both IMIOPC and AMIOPC.[6] Currently, there is no Marine Corps MOS or MAGTF-specific training associated with MILDEC, OPSEC, or SIGMAN outside of IMIOPC and AMIOPC. Currently, AMIOPC provides the identical MILDEC and OPSEC training that is mandated by the Joint Staff J-39 and delivered by the Joint Forces Staff College—except that AMIOPC is taught using a MAGTF-specific training scenario. Also of special note, the OPSEC planning process is taught from the operational perspective that integrates OPSEC into the operational plan to aid the commander achieve tactical and operational objectives—not the "Halls and Walls" OPSEC program managers course, which has its place but does not necessarily teach planners what they need to know to plan, execute, and assess OPSEC and SIGMAN on the battlefield.

Adjustments have to be made once execution begins to ensure operational success. *(Photo by Cpl Cutler Brice.)*

The third newly proposed T&R manual functional area is execution. Execution is all about what happens when the plan passes from future operations to current operations and the actions an OIE practitioner must do to ensure that the measures of performance are being executed in accordance with (IAW) the synchronization matrix. It also entails how adjustments are made to ensure operational success after the adversary begins to execute their plan and simultaneously adapt to ours. Currently, transitioning plans from future operations to current operations is knowledge acquired on-the-job by someone who has recently been trained as an OIE planner, but with little experience with its actual execution. This knowledge deficit creates a massive learning curve for the practitioner, especially because it is difficult to practice OIE execution in a garrison environment without a robust synthetic training environment. An OIE practitioner at all levels should learn about information as it relates to current operations, development of battle drills, participating in the targeting process, and execution of the synchronization matrix. At the intermediate level, an OIE student should learn about authorities and permissions and how to go about putting them in place. At the advanced level, students should get an in-depth study of the deliberate and dynamic land component and joint targeting processes, how they work, and methods for OIE integration.

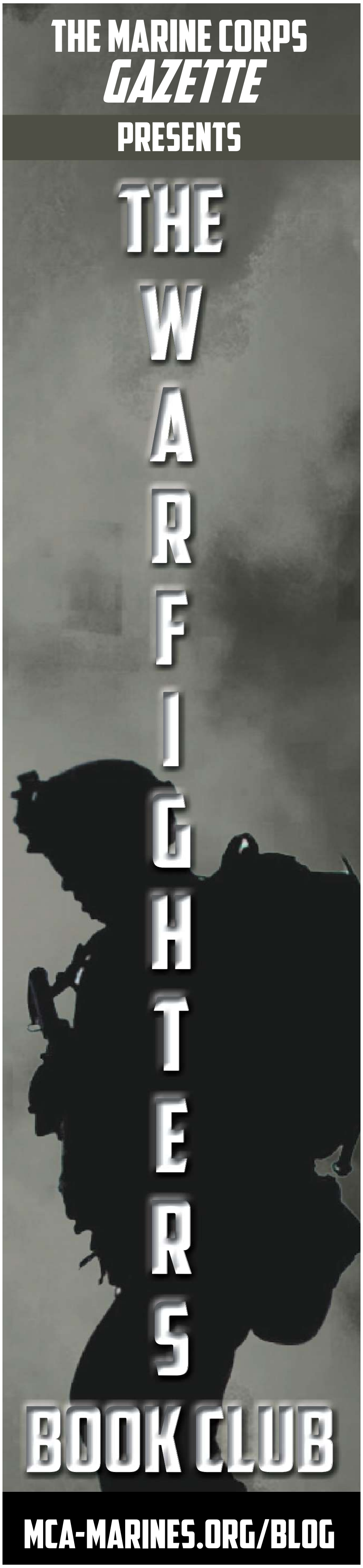
The fourth newly proposed T&R manual functional area, assessment of OIE plans and activities, is arguably the most important and most neglected function for an OIE practitioner. The assessment of plans and activities is an extremely challenging task since the information environment is influenced by many different factors, which lead to an extremely subjective process. Oftentimes in the past, the difficulties developing meaningful measures of effectiveness have resulted in a loss of confidence by commanders in their OIE efforts. Also it is possible that many scarce resources have been squandered without any real evidence demonstrating that planned information environment actions have actually created the desired effect. At the intermediate level, students should learn the joint IOs assessment framework and the intermediate target assessment process. At the advanced level, Marines should dive deep into the behavior sciences and measures of progress in a conflict environment as an approach to targeting assessment. Systems analysis and operations research techniques should also be taught so that OIE practitioners can develop operational assessment frameworks for their information concepts of support, implement scientific methods and instruments to survey the information environment, and ultimately provide the skills to analyze data and other assessment activity results. Finally, students should be exposed to national, joint, and Marine Corps intelligence systems for familiarity with intelligence, surveillance, and reconnaissance planning and asset utilization as well as other joint tools available for assessment purposes.

Recommendations

Ultimately, it is the responsibility of the FMF to understand the information environment and effectively employ their OIE practitioners and information forces to achieve operational advantages over our current and future adversaries. However, even more importantly, at a time when our adversaries are rapidly expanding their abilities to dominate the information environment, it is incumbent upon the Marine Corps to do the same and thoroughly prepare its Marines who are assigned to critical OIE and information capabilitiy billets throughout the FMF. As a result, the Marine Corps should take the following actions with regard to preparing its Marines to fight and win in the information environment:

- Expand IMIOPC (corporal to lieutenant colonel, MOS 0510 and MOS 0551) and AMIOPC (1st lieutenant to major, MOS 0550) IAW the recommendations outlined above, including instruction on the latest OIE concepts, functions, and capabilities as well as current and projected information warfare threats.
- Expand IMIOPC (gunnery sergeant to major) to at least a four-week program of instruction (POI) IAW a detailed learning analysis resulting from the T&R manual tasks outlined above.
- Create a Basic MAGTF IO Practitioner Course (BMIOPC, corporal to gunnery sergeant) POI for enlisted IO specialists to train to unique 0551 T&R manual conditions and standards.
- Incorporate advanced wargaming with well-trained adversary red cells and information environment modeling and simulation analysis techniques in the BMIOPC, IMIOPC, and AMIOPC POIs.
- Make AMIOPC a top secret/special compartmental information-level course. Incorporate alternate compensatory control measure read-ins, combatant command operations plan reviews, as well as common access billet read-in for special technical operations planning for AMIOPC students. Incorporate and fund field trips and studies of key Marine Corps OIE commands, agencies, centers, and groups as well as other service and national-level IO, space, cyber, and intelligence capabilities.
- Integrate C2 of information environment and information environment battlespace awareness capabilities and technologies immediately into BMIOPC, IMIOPC, and AMIOPC as they are fielded as well as emerging MEF information group combat operations center processes and procedures.
- Ensure all Marines filling OIE FMOS billets receive BMIOPC, IMIOPC, or AMIOPC training in route to their assignments.
- Consider removing the OIE FMOSs from the 05XX MAGTF Plans series since OIE and information warfighting functions are far more than planning functions.
- Explore options to retain critical OIE officer knowledge, skills, and experience through creating a PMOS or alternate reutilization assignment strategies.
    - Create an OIE PMOS for information capability MOSs (Cyberspace Operations, Space Operations, electronic warfare, PSYOP, and Civil Affairs) after the rank of captain/sergeant, similar to the 02XX model that funnels officers into the 0202 MOS.
    - Use a secondary MOS model where officers and enlisted Marines alternate tours between their primary OIE/Information Capability

We must be able to achieve an operational advantage over our enemy. ***(Photo by Cpl Malik Daniel.)***



MOS and IO FMOS (0510, 0550, and 0551) after the rank of captain/sergeant. This concept also includes the Special Education Program Technical IO Officer MOS 8834 as well.

- Consider expanding upon the model outlined in this initiative and create an OIE Weapons Tactics Instructor (WTI) model similar to the Marine Aviation Weapons and Tactics Squadron-1 (MAWTS-1), Marine Corps Tactical and Operations Group, and Marine Corps Logistics and Operations Group paradigm for post 0550, Advanced IO Officers. This would also align with the naval Information Warfare Development Command's current initiative to create Navy information warfare tactics instructors. We recommend the Marine Corps IOs Center be the location of Marine OIE WTI training but closely integrated with MAWTS-1, Marine Corps Tactical and Operations Group, and Marine Corps Logistics and Operations Group.
- Enter into a formal agreement between Navy Information Forces, naval information warfare development command's and the Deputy Commandant for Information to integrate Navy information warfare and Marine OIE WTI training across the naval Services in support of the *Commandant's Planning Guidance*, *Littoral Operations in a Contested Environment*, *Expeditionary Advanced Base Operations,* and *Distributed Maritime Operations*.

Conclusion

At this time, because of the ongoing force design process, it is uncertain exactly how the Marine Corps will transform its OIE force. Nevertheless, the need for a dedicated and experienced cadre of OIE practitioners will continue to grow as our adversaries continue to refine their use of the information environment. At a time when our adversaries are rapidly expanding their abilities to collect, process, and disseminate information within the information environment, with the aim of influencing and imposing their will on their adversaries, it is critical that the Marine Corps do the same. While it is the responsibility of the FMF to employ OIE practitioners effectively, the training establishment must ensure these information warriors have the knowledge and skills required to successfully fight and win throughout this highly contested domain. Lastly, in order to ensure that the Marine Corps stays ahead of our adversaries, Expeditionary Warfare Training Group, Atlantic, partnered with Deputy Commandant for Information, is already focused on implementing the necessary and crucial changes to enable our OIE professionals to dominate this increasingly important domain throughout the entire cooperation, competition, and crisis continuum.

Notes

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

[2] James R. Clapper, *Opening Statement to the Worldwide Threat Assessment Hearing, Senate Armed Services Committee*, (Washington, DC: February 2016), available at www.dni.gov.

[3] Larry M. Wortzel, *The Chinese People's Liberation Army and Information Warfare,* (Carlisle, PA: Strategic Studies Institute, March 2014), available at www.strategicstudiesinstitute.army.mil. This study examines China's efforts in implementing information warfare with advanced technologies while expanding the air defense intercept zone.

[4] Jolanta Darczewkska, *The Anatomy of Russian Information Warfare,* (Warsaw: Centre for Eastern Studies, May 2014), available at www.osw.waw.pl. This paper examines the changing techniques of Russian information warfare, in respect to the recent Crimean operation.

[5] Currently, U.S. Army, Navy, and Air Force personnel serving in the IO field remain in that field throughout their careers. Refer to *DA-PAM 600-3, NEOCS Manual* Volume 2, and AFECD, respectively.

[6] Headquarters Marine Corps, *MCRP 3-32.2, Multiservice Tactics, Techniques, and Procedures for Military Deception (MILDEC) Operations,* (Washington, DC: 2012); and Joint Staff, *JP 3-13.3, Operations Security,* (Washington, DC: 2012). These are the primary military deception and operational security publications upon which the new curriculum should be built.

Revolution in Military Affairs

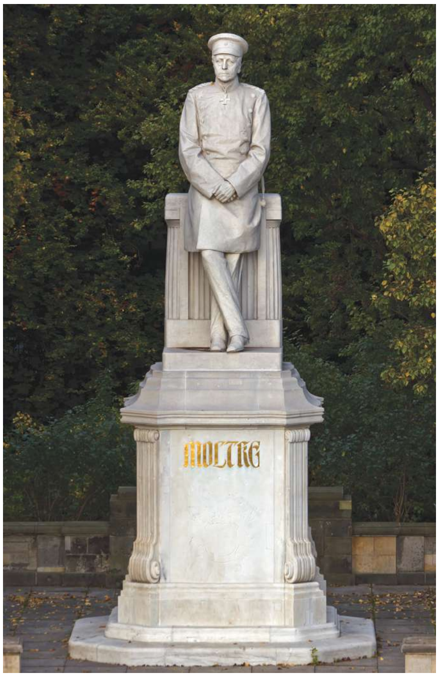
Parallels of 18th and 19th century tactics and technologies to 21st century cyberspace operations

by LtCol Jamel Neville

>LtCol Neville is a 1702 Cyberspace Officer.

While the cyberspace domain changes how today's global superpowers compete militarily, parallels and insights can be gleaned from the revolutions in military affairs over the past two centuries. In the late eighteenth century and throughout the nineteenth century, the French Revolution, Napoleonic Wars, and Industrial Revolution shifted the ways and means in which battles were fought and won between nation-states. The French Revolution demonstrated the value of the citizen soldier and national armies over episodic formations. This value, coupled with Napoleon's employment of non-traditional maneuver tactics and kinetic fires, made France a formidable threat within Europe during the Napoleonic Wars (1803–1815). The Royal Prussian Army's Field Marshal Helmut von Moltke further advanced maneuver warfare concepts through the establishment of the general staff, empowerment of subordinate commanders at the tactical level, and exploitation of the introduction of locomotive technology throughout the nineteenth century.

Napoleon; (Painting by Jacques-Louis David, 1748-1825.)



Helmut von Motlke, the Elder. (Photo by A. Savin.)

As the world transitioned from the Industrial Age to the Information Age throughout the twentieth century, the United States enjoyed a notable competitive advantage in the cyberspace domain following its invention of the Internet. However, over the past two decades, nation-states, to include Russia, China, Iran, and North Korea have expanded their cyberspace capabilities to be on par with the United States.

Nineteenth century military sea and land operations, French Army shortcomings and the successes of the Prussian Army provide joint and MAGTF commanders, operational planners, and cyberspace operations forces (cyber warriors) historical references for planning and directing cyberspace operations. While Napoleon's maneuver warfare tactics provided him with a competitive advantage, these successes were short-lived. Moltke's advancement of maneuver warfare concepts through reformations of the Prussian Army are worth noting. He placed a premium on training and education, optimized command and staff operations, and capitalized on the technological shifts of the Industrial Revolution. These reformations ultimately changed the character and nature of warfare well into the twentieth century.

Warfare has shifted from the deployments and maneuvering of large formations at the level of total war (e.g., World Wars I and II) to the persistent, multi-domain operations of today. From Russia's employment of cyberspace effects to enable "gray zone" operations and disinformation campaigns; China's routine acts of cyberespionage; to Iran and North Korean conducting sophisticated cyber-attacks over the past decade, U.S. adversaries are leveraging the cyberspace domain to increase their legitimacy on the world stage. Adversarial threats will continue to persist within cyberspace and become more complex. Joint and MAGTF commanders and operational planners must understand how to effectively employ cyber warriors against these threats, and integrate cyber capabilities to enable the lethality across multi-domain operations.

Napoleonic Wars

Throughout the late eighteenth and into the nineteenth century, nation-states primarily employed frontal attacking formations. Battles were fought in stages (e.g., artillery, following by infantry and cavalry, etc.). Napoleon annihilated European armies by employing non-traditional tactics to include light, maneuverable infantry formations to envelop opposing armies. Enabled with supporting combat arms (i.e., artillery), Napoleon massed the preponderance of his forces and fires against an opponent's center of gravity, at the time and place of his choosing.

While there are many advantages to Napoleon's maneuver and combined arms tactics for joint and MAGTF commanders and cyber warriors to reflect upon, it must also be noted that Napoleon's centralized command and control model resulted in his failure. "Napoleon insisted not only on one-man rule but also on one-man command, the operational core of his staff was never more than an organization for assembling information he required and for transmitting reports and orders," according to Peter Paret in "Napoleon and the Revolutionary War" in *Makers in Modern Strategy*.[1] Napoleon's centralized command and control model impeded his ability to wage war as nation-states' armies grew and became more geographically dispersed. The increase in force disposition–under a single commander–ultimately resulted in a series of French defeats by *coalitions* of European nations between 1808 and 1815. While Russia, China, Iran, and North Korea have increased their cyberspace capabilities, authoritarian states lack the advantage of strong coalitions such as the United States and its Five Eye (FVEY [Australia, Canada, New Zealand, the United Kingdom, and the United States]), North Atlantic Treaty Organization (NATO), and Association of South East Asian Nations (ASEAN) partners. These relationships provide the joint or MAGTF commander the ability to potentially leverage additional authorities or resources required to effectively execute cyberspace operations.

> ***... Napoleon's centralized command and control model resulted in his failure.***

Moltke and the Royal Prussian Army General Staff

The Royal Prussia Army gleaned lessons and insights from the Napoleonic Wars and instituted a series of reforms to further mature the concept of maneuver warfare. These reforms included refining envelopment tactics and introducing the *mission command* model. The Prussian general staff was comprised of a group of officers who were empowered to develop military operational plans, executed by subordinate commanders at the tactical level. "Moltke transformed the Prussian general staff into a unique instrument combining flexibility and initiative at the local level with conformity to a common operational doctrine and to the intentions of the high command," according to Gunther Rothenberg.[2] The mission command model enabled Prussian tactical commanders to make decisions at their level, which yielded better operational outcomes.

Being selected to serve on the Prussian general staff represented a great accomplishment, for it was staffed with the most highly qualified officers. Moltke further matured Napoleon's merit-based system by requiring all general staff members to complete professional military education. A disciple of Clausewitz and inspired by the tactics of Napoleon, Moltke sought and encouraged critical thinking and decision making. All officers completed *Kreigsakademie* (War College) prior to serving on the general staff and as a prerequisite for field command. He fostered a culture of life-long learning through a variety of continuous staff training and instruction. "[Moltke] schooled the [general staff] to think through the problem of attaining the end of strategy through the conduct of operations. He used this operational conduct as a level

Cyberspace operations are intelligence-driven. ***(Photo by SSgt Jacob D. Osborne.)***

Cyber warriors should operate with an offensive mindset. *(Photo by SSgt Jacob D. Osborne.)*

for achieving the strategic goal," according to Michael Krause.[3]

The Industrial Revolution birthed the train and railway system. The technology increased lines of communication and decreased the tyranny of distance in the land domain. While Napoleon's principle of maximizing the preponderance of forces and fires at an opponents' centers of gravity, the introduction of the locomotive enabled Moltke and the Prussian general staff to facilitate these conditions more rapidly and over greater distances. As noted by Paret,

> [t]roops could be transported six times as fast as the armies of Napoleon had marched, and the fundamentals of all strategy—time and space—appeared in new light … The speed of the mobilization and of the concentration of armies became an essential factor in strategic calculations.[4]

Rather than analyzing the locomotive capabilities in isolation, Moltke and the Prussian general staff creatively integrated its capabilities to further enhance existing military capabilities (i.e., forces and fires) and plans to achieve Prussia's strategic military aims. Joint and MAGTF commanders and cyber warriors should view and employ cyberspace capabilities in the same manner.

Creativity, foresight, and ingenuity are what set Moltke apart and gave the Prussian Army its competitive advantage throughout the nineteenth century. The result was an elite corps of Prussian Army planners, empowered to think critically and develop solutions in a decentralized manner. Commanders and staffs should glean from this principle by continuously working to bring cyber warriors' collective intellectual capital to bear and exploring the art of the possible in the cyberspace domain. Cyber warriors should not only be highly trained technicians and critical thinkers, but their tradecraft must be intelligence-driven. Cyber warriors must understand *how* existing and emerging defensive and offensive cyberspace capabilities enable favorable operational and strategic outcomes. Moreover, given the joint interdependence and strategic impacts of cyberspace operations, cyber warriors should be able to effectively lead people, collaborate, and interoperate with multiple stakeholders.

Final thoughts

A key advantage that the United States has over authoritarian states is its fostering innovation and ideas for the greater good of society, such as the invention of the Internet. However, the United States must not be naïve or grow complacent as unprincipled global actors continue to leverage the Internet to undermine and threaten democracy and national security.

Cyber warriors should operate with an offensive mindset and persistently explore the *art of the possible* when planning and conducting cyberspace operations against adversarial threats. Joint and MAGTF commanders and operational planners must ensure cyber warriors are well-trained and empowered to innovate and develop cyber warfighting excellence. Innovative thinking increases within teams and organizations as leaders develop a culture of trust, empower people, and effectively manage talent. Cyber warriors must be challenged and given a sense of purpose to ensure the Joint Force remains postured to *fight and win* in the cyberspace domain. The study of Moltke and his development of the Prussian general staff is a noteworthy example.

Finally, commanders must realize that cyberspace operations are a *joint* fight with little to no separation between the tactical and strategic levels of military operations. Despite Napoleon's dominance, he was ultimately defeated by a *coalition* of countries. The United States' strategic partnerships with its FVEY, NATO, and ASEAN partners are key to enabling global offensive and defensive cyberspace operations in support of national security objectives.

USMC

Notes

[1] Peter Paret, "Napoleon and the Revolutionary War," *Makers of Modern Strategy,* (Princeton, NJ: Princeton University Press, 1986).

[2] Gunther E. Rothenberg, "Moltke, Schlieffen and the Doctrine of Strategic Envelopment," *Makers of Modern Strategy,* (Princeton, NJ: Princeton University Press, 1986), 301.

[3] Michael D. Krause, "Moltke and the Origins of the Operational Level of War," *Historical Perspectives of the Operational Art,* (Washington, DC: Center for Military History, 2005).

[4] "Napoleon and the Revolutionary War."

Who Needs COMMSTRAT?

How an improved Fleet Marine Force leadership structure and improved communication strategy and operations better supports the warfighter

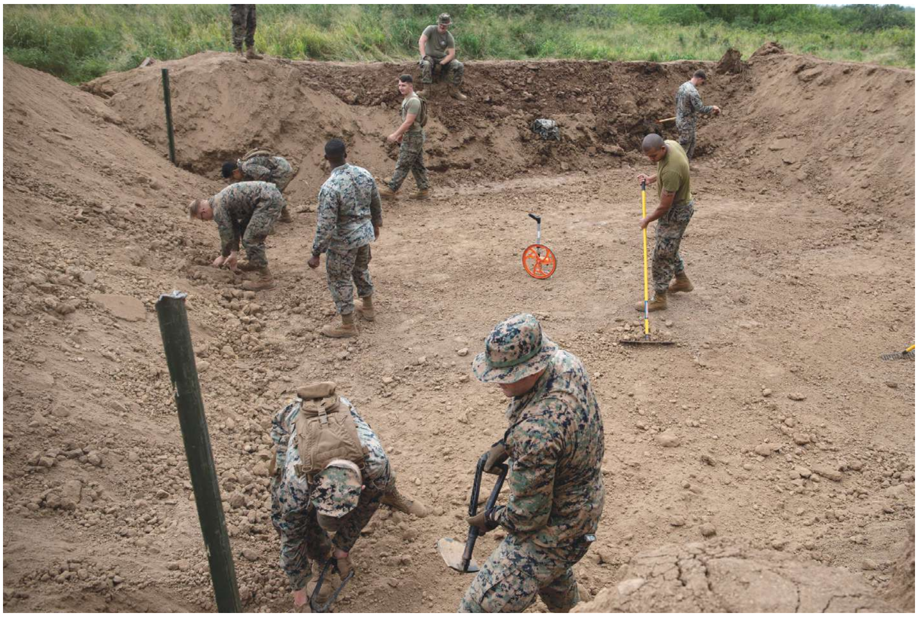
by Capt John J. Parry

>Capt Parry is a Communication Strategy and Operations Officer and currently a student at Expeditionary Warfare School. He has served tours during Operation ENDURING FREEDOM and OAKEN LOTUS, and with Marine Corps Forces Korea, II MEF, the School of Infantry, and the Communication Directorate.

Communication strategy and operations (COMMSTRAT) serves as the "backbone" of the message and visual information production support for the MAGTF. As a supporting capability within the new seventh Marine Corps warfighting function of information, the COMMSTRAT community has a problem set that will improve the speed and focus of the MAGTF once solved.[1] This problem set includes identifying and delineating roles and responsibilities between the Fleet Marine Force (FMF) and Supporting Establishment (SE) while optimizing operational structure for COMMSTRAT forces. The lack of a unifying concept for the public affairs and combat camera merger has left COMMSTRAT Marines reeling to understand what the new occupational field (OccFld) needs to do to make this happen. This stems from the rapid merger of the legacy public affairs and combat camera fields which began in 2016. The merger led to the emergence of the COMMSTRAT OccFld, but no new policy or doctrine related to the merge followed in trace.

Over the past decade, the OccFld has continued to remain relatively unhealthy at the senior ranks.[2] This deficit in leadership and personnel as a whole actually drove the Service's decision to execute the merger. Another symptom of the problem is the lack of structure to nurture proficiency and develop leaders for the senior ranks. Junior company grade officers continue to face a future where they enter the fleet and have no "top cover" in working directly for a chief of staff and general officer in their first billet. No other OccFld has second lieutenants working at senior commands as the senior advisor for their community. Both a cause and symptom of the problem, the community has a significant deficit in the lieutenant colonel and colonel ranks, which degrades the ability of the community to teach, coach, mentor, and choose with whom to invest from the junior ranks. These gaps make it particularly challenging for the COMMSTRAT Marines supporting the range of military operations, considering they are one of the few MAGTF capabilities continuously working to shape the operating environment even while their peer organizations are solely focused on training and readiness.

The Marine Corps' leadership definitely understands the need for COMMSTRAT capability, having supported precepts for promotion boards to protect



COMMSTRAT is continuously working to get the Marine story out. *(Photo by LCpl Samantha Sanchez.)*

the OccFld, but this has not translated at the operational and tactical levels in the FMF. In order to fix the problem, the COMMSTRAT OccFld needs to improve its organizational leadership structure and competitiveness, which ultimately improves support for the warfighter. The community can also make significant strides in improving operational support with better definition of FMF and SE roles and responsibilities, which supports improved efficiency, force proficiency and development, and warfighting effectiveness.

Roles and Responsibilities for COMMSTRAT: FMF vs SE

The Marine Corps can improve its COMMSTRAT support for the warfighter with a better understanding of "who does what" between the FMF and SE. The whole purpose of the FMF in garrison is to prepare for war. The purpose of the SE is to support the warfighter and enable his ability to prepare for war. The most significant problem with the OccFld stems from the blur between roles and responsibilities in the FMF versus the SE.[3] What COMMSTRAT needs to define for the FMF is how it will support all the information-related capabilities' production demands for communication products while in execution of any of the range of military operations. This means focusing on targeted audiences, how they receive their information, and generating products and engagements to reach them the way they will best receive it.

A focus on training and supporting training for command and control capability is the best way to make this happen. Legacy FMF public affairs operations in garrison focused on production of visual information products (VIPS), which generally had little reach and impact. The targeted audience for a unit conducting training on a local range, which was historically the FMF garrison main effort, is limited or negligible. The "so what" of garrison generated VIPS ultimately feels that it is aimed toward getting the attention of senior leadership. This serves little value to the enterprise. In the past, at least, units had their picture on the front page of a base newspaper, which many senior leaders said was not worth their time. When I was a second lieutenant, for example, my battalion commander told me upon seeing his unit on the front page of the base paper, "That's good fish wrap." Now those pictures are posted on official unit web pages, which garner marginal interest. Current traffic usually includes new Marines checking into a unit and searching for contact information, or by Marines who are searching for a link to outlook web access or SharePoint. Granted, garrison unit training stories on targeted communication mediums can provide value to a unit when they focus on the accomplishments of individual Marines (see note below on UIO program).[4] Yet, COMMSTRAT Marines do not have the capacity to support all units down to the platoon level while building the proficiency required for war. FMF COMMSTRAT should still generate VIPS; however, the value and priority should be on the training these events provide for COMMSTRAT forces to support the ROMO. Much of the legacy combat camera print mission and equipment also needs to go to the SE. This includes print and reproduction capability outside of deployable systems, posters, and other methods. Many requests for internal products are a "nice to have" for the FMF and not a requirement. Nice to have is not expeditionary. These requests require expensive and facility consuming non-expeditionary equipment that will not go with the warfighter when the order comes from higher headquarters. Additionally, the Marine Corps demands an "expeditionary" mindset, which means all supporting arms capabilities must minimize their required space aboard ship for combat deployments to maximize space for personnel, vehicles, aircraft, and life support. Legacy combat camera support to the warfighter should focus on documentation, staff VIP support requests, and deployable print support capability.[5] All information operations and staff support requests for FMF COMMSTRAT in garrison should be supportable to the extent that capability can go forward. The SE can fulfill any other requirements for the FMF.

Improved Support to the Warfighter

The Marine Corps can improve its support for the warfighter by economizing COMMSTRAT forces while in garrison. This means structuring and focusing FMF COMMSTRAT capability where it is actually needed as Marine forces provide support to the unified commands. It also means economizing COMMSTRAT forces by moving them from the MEF command element (MEF CE) and main supporting commands (MSCs) and then allocating and reorganizing them at the MEF information groups (MIG). This supports a proposed principle that COMMSTRAT staffs use COMMSTRAT products and services while COMMSTRAT organizations produce them. This principle drove planning for the intel OccFld in the 1990s and also mirrors the design of other MIG enabler battalions. While this principle does mean a reduction of personnel in garrison at the MEF CE and MSCs, it also means ownership of the right capability within the MEF CE and MSCs to ensure support for global force management and proper identification of ready, scalable COMMSTRAT forces attached via the MIG to serve the ROMO. The MEF CE will plan and provide oversight of all FMF COMMSTRAT through leading global force management and the command inspection program.[6] The MIG will ensure the readiness of COMMSTRAT production and service support to the MEF CE and MSCs. The COMMSTRAT capability will realign and reorganize at the MIG, which improves support for the current Combat Development & Integration concept for MAGTF information environment operations concept of employment.[7] The staffs at the MEF CE and MSCs can then use COMMSTRAT products and services while the MIG COMMSTRAT capability produces them. MEF CE and MSC leaders will then require the following capabilities from COMMSTRAT in garrison:

- Public affairs advisor.
- Plans, future operations, current operations capacity.
- Media engagement.
- Communication medium supervision and training (marines.mil websites/social media).

- Unit information officer program implementation and oversight.

I argue that these are the actual requirements for FMF COMMSTRAT capability in garrison even with the current allocation of forces. The reduction in garrison MEF/MSC COMMSTRAT forces will allow the Marine Corps to apply economy of force toward garrison requirements. The realigned COMMSTRAT forces at the MIG will provide scalable, task organized capability to the MEF and MSCs for deployments or development of VIPS as required (crisis communication, law enforcement, good news stories). Many public affairs officers have long argued that at the beginning of Operation Iraqi Freedom, the MSCs did not know their staff. All public affairs personnel at this time were consolidated at the SE. The above proposed construct ensures organic senior leadership at the MEF/MSC level who maintain the right capability to mitigate this gap in trust. The staff assigned to the MEF CE and MSC COMMSTRAT staffs will lead COMMSTRAT teams allocated to them by the MIG, whose teams will have been validated through training and exercises. These teams will also maintain a general or direct support command relationship in garrison.

The reduction in garrison requirements for the FMF will enable the reorganization of tactical COMMSTRAT forces, which nearly triples the number of COMMSTRAT operational support teams (i.e., a COMMSTRAT platoon) at the MIG. This COMMSTRAT company will then become a battalion with three companies. The battalion will have a command-slated battalion commander and senior enlisted leader from the community. The companies will have a company commander and senior enlisted leader from the community. The company will have three platoons led by a platoon commander and platoon sergeant. The proposed structure will require no additional staff. The new MEF support battalion will provide the S-shop functions required to provide the unit life support in garrison. This is a proven model, which is currently used at the School of Infantry-East to support the training battalions. (I also argue that the Service can even look to consolidate the other S-functions from the enabler battalions at the MEF support battalion for greater efficiency.) The Marines within the COMMSTRAT company will support the MIG, MEF CE, and MSC requirements while maintaining focus on training and readiness as the main effort. Training and readiness has never been a focus for COMMSTRAT forces. The legacy public affairs and combat camera communities assumed to an extent they were trained and ready because of a largely self-induced—and not necessarily required or relevant—operational tempo in garrison. The focus on training and readiness will improve the quality of COMMSTRAT support to the warfighter.

Training and readiness will still be the focus. *(Photo by LCpl Nicolas Atehortua.)*

Improved COMMSTRAT Leadership Development

The realigned FMF structure will improve the structure for developing junior Marines and improve competitiveness for both enlisted and officers among their peers. Historically, officers and SNCOs in both public affairs and combat camera had little interaction at their commands with senior OccFld Marines. This "spread the peanut butter thin" concept made public affairs and combat camera Marines a lot like an octopus. The octopus is the smartest non-vertebrae in the ocean. However, it has a fatal flaw. The octopus does not nurture its young. When the octopus dies, the knowledge it accrued over its lifetime dies with it. Instead, the previously proposed COMMSTRAT organization enables senior COMMSTRAT leaders to nurture the leadership and professional abilities of younger Marines and pass on their hard-earned knowledge. The proposed structure empowers COMMSTRAT Marines to demonstrate leadership ability, compete with their peers, and the ability to identify and shape the next generation. The new structure will foster a "boss" or "commander's mentality." I also add that a commander's mentality is far different from a "staff mentality," whereas the commander must focus on his responsibility for the whole command while the staff focuses solely on their specialty. A COMMSTRAT Marine with experience as a commander will better understand the challenge of command and improve support in such a way that only an experienced commander would. The proposed shift in focus will improve the quality of COMMSTRAT support to Marine Corps warfighting where it counts the most: operations across the range of military operations in support of their command, the unified commands, and the United States of America.

This article provides a solution for the FMF to improve the operational design of the COMMSTRAT OccFld. Consolidation of COMMSTRAT assets and clearly defined FMF/SE roles and responsibilities help ensure the Marine Corps builds upon its reputation as the finest warfighting organization in the world. Nonetheless, the COMMSTRAT OccFld needs the buy-in of senior leaders to improve support to the warfighter, and improve the OccFld's professional development and competitiveness.

Notes

[1] Headquarters Marine Corps, *CMC White Paper*, (Washington, DC: January 2019).

[2] Headquarters Marine Corps, Manpower & Reserve Affairs, *MMPR/CEB Statistics for FY19*, (Washington, DC: 2018).

[3] Headquarters Marine Corps, *MCO 5720.77, Marine Corps Public Affairs Order*, (Washington, DC: July 2010). See also Headquarters Marine Corps, *MCO 3104.1B, Marine Corps Combat Camera Program*, (Washington, DC: October 2011). These orders do not define the new occfield requirements and instead focus on the competing requirements between Public Affairs and Combat Camera. There is no unifying order, policy, doctrine, or concept for the COMMSTRAT occfiield.

[4] Recognition of the individual Marine will become the responsibility of the command to which he belongs. The Unit Information Officer program is designed to be overseen by the MEF and MSC CommStrat capability and handled at the small unit level by an officer of the command's choosing. This remains an important aspect of building trust and camaraderie within a command. CommStrat does not have enough Marines to show recognition of every Marine's awards and promotions. However, CommStrat can train unit information officers to generate this information and manage their command's communication mediums. See *MCO 5720.77* for details.

[5] Ibid.

[6] This program does not yet exist.

[7] Headquarters Marine Corps, *Marine Air-Ground Task Force Information Environment Operations Concept of Employment, Combat Development & Integration*, (Washington, DC: July 2017).

>*Editor's Note:* See MARADMIN 004-20, Announcement of Way Ahead for Reestablishing/Reinvigorating Fleet Marine Force and Navy-Marine Corps Componet Command Relationship, (Washington, DC: January 2020).

Talent Management for Cyber Warfare

Maintaining the right workforce

by Capt Aric A. Ramsey

>Capt Ramsey is a Communications Officer serving as a Service cyber protection team leader attached to the Marine Corps Cyberspace Operations Group.

The means and methods the Marine Corps uses to fight its battles are rapidly changing. Each warfighting function is increasingly dependent on cyberspace for the speed and flexibility it generates through shortening the decision-making process and enabling more efficient prosecution of innumerable tasks. In its heavy reliance on digital data, the service is accepting highly targetable critical vulnerabilities in cyberspace, which are compounded by the Service's deep-rooted culture of making data available over keeping it secure. This system of systems, touted as a critical component of U.S. strength, has already become a fairly easy, low-cost, high-payoff target for our global competitors. Recent examples of U.S. government network vulnerabilities, such as the Office of Personnel Management breach of 21.5 million personal records or the penetration into the Joint Chiefs network, remind us that the threat of attack in and through cyberspace is real and underscores the inevitability of network compromise.[1] Thus our dependence on cyberspace, along with the struggle to keep up with potential adversaries in that domain, are subjects of much interest within the Department of Defense (DoD).[2] At the same time, the DoD faces problems maintaining a workforce of sufficient size and skill to support cyber operations, which fundamentally undermines efforts to operate effectively and securely in cyberspace. These manpower issues are well known and documented to some extent. Several years ago, the DOD published a cyberspace workforce strategy that identified the need for better recruiting, evaluation of skill maturity, and retention of qualified personnel—among other concerns.[3] The recommendations presented were generic and lacked realistic application, and the DOD still faces many of these same issues today. Unfortunately, the problem especially impacts the Marine Corps which lags behind its sister services in taking corrective action. The current Commandant is rightly interested in the Marine Corps' systemic talent retention problem, suggesting an incentives-based model that uses money like a focused weapon aimed exactly at the individuals we need.[4] The coming year will serve as a good indicator of whether his guidance will result in stemming the talent hemorrhage plaguing many specialized occupational fields. While not a panacea, making the cyber warfare community the first among such incentive-targets will close significant inequalities in pay and thereby remove one of the major considerations prompting young and qualified Marines to take the skills the Marine Corps has sacrificed to cultivate over to other uniformed services or the civilian workforce.

The methods used to fight in the future will require cyber operator skills. (Photo by Cpl Victoria Decker.)

Cyber warfare is by nature a human-centric endeavor requiring highly trained and professional forces. The Marine Corps recognizes this and has made significant investment in the people it places in cyber warfare billets.

As we enter into the nineteenth year of the U.S. Cyber Command force building effort, a large amount of our most talented operators continue to exit the Marine Corps well before retirement. There are two primary reasons for this. First, Marines practicing cyberspace operations have few opportunities to be hard-living Marines, instead "engaging" with our nation's enemies through a laptop while seated in a cubicle and tucked in a secure building. This is not how recruits imagine Marine Corps life to be. Second, employment in the commercial cybersecurity industry requires certifications and experience, and our cyber-billeted Marines are equipped with both of these early in their careers. This makes them extremely competitive in the commercial industry at an average starting salary of $116,000.[5] On top of this extrinsic reward, the civilian world has no barracks inspections, no bailing coworkers out of jail at 0200, no mandatory change of station orders, no monthly 24-hour duties, and even allows its employees to use hotplates and rice cookers in their living quarters. Now the Corps is fielding its new 17XX occupational field of Marines, turning from the current paradigm of periodically rotating personnel back to communications or intelligence units to one where they will exclusively conduct cyber operations at the national or Marine Expeditionary Force level. This move was designed to stop pulling talented Marines from a highly specialized job just as they were achieving proficiency. It is likely to have an unexpected and profoundly negative effect on retention, as Marines are vertically assessed out of boot camp and immediately given at least 4 years of experience, a hundred thousand dollars in education, and a top-secret clearance. While nothing should be done about the inherently unpleasant aspects of being a Marine, something must be done to appropriately reward the high-demand, low-density skills of the Marines conducting cyber operations.

The current solution to cyber force staffing involves hiring contractors and federal service (GS and GG) employees to serve alongside Marines. This move not only enabled the Marine Corps to reach staffing goals faster than it could produce qualified uniformed operators, it also intends to provide continuity by building long-term expertise through years of service in the same job or command, whereas Marines transition frequently. Yet civilians often provide even less continuity than Marines. Because they receive the same training but have no contract to honor, civilians have the freedom to leave with merely two weeks' notice. In the new and rapidly developing field of cyber warfare, there is no shortage of attractive job offers within the Cyber Mission Force (CMF) that tempt employees to continuously transition jobs and rapidly climb the ladder to increased salaries. Additionally, a civilian is only allowed to work a 40-hour week. If they are asked to work more, they must receive additional time off or overtime. Finally, Federal employees in the GS-12 and 13 grade (step 5), who currently comprise a significant segment of the civilian cyber workforce, earn an annual salary of $94,520 and $112,393 respectively with access to competitive healthcare plans available for approximately $8,000 per year in premiums.[6] In comparison, a staff sergeant with 12 years of service, who comprise a significant segment of the uniformed cyber workforce, earn approximately $65,266 annually, including basic allowance for housing.[7] It is worth noting that this comparison between GS and military comparison is conservative. Marines who choose to enter the contracting force or private industry can reasonably expect to earn even more, although the tradeoff is often job security. In addition to an approximate $18,000 disparity in annual pay, Marines are regularly required to work longer hours, to include weekends, while civilians are required to leave after they reach their standard hours for the week, except in the extreme case where overtime is authorized. Collectively, these discrepancies naturally sow tension between the Marines and civilians working side by side, providing additional motivation and means for qualified Marines to leave the uniformed service. This is not intended as an indictment against our dedicated civilians. Rather, it is the unfortunate result of fundamentally different human resource models that cannot and should not be reconciled but are forced to co-exist. With whom is the uniformed cyber warfare community left? It is left with those few, highly qualified patriots for whom the intrinsic reward of service to the Corps is sufficient, those who have laterally moved into the community late in their career and are now a few years away from retirement, and those whose prospects in industry are less than promising.

The problem of retaining the most qualified and skilled Marines in cyber warfare billets is not new. In 2015, then Secretary of Defense Ash Carter proposed loosening standards on recruits who come with certain industry standard qualifications to boost the technical capability of the Service.[8] He posited that since cyber warfare is not conducted in the physical domain, recruits entering a cyber MOS should not be held to physical fitness standards and could potentially be exempted from attending boot camp. This concept, known as "lateral entry," was echoed by then MajGen Lori Reynolds, who compared the way the Marine Corps band is staffed with the potential future of the Marine cyber warfare workforce, though she later suggested that the Marine Corps will not change the culture of first being a Marine, then a rifleman, and finally a cyber warrior.[9] According to then MajGen Loretta Reynolds during the 2017 Navy League Sea, Air and Space Exposition:

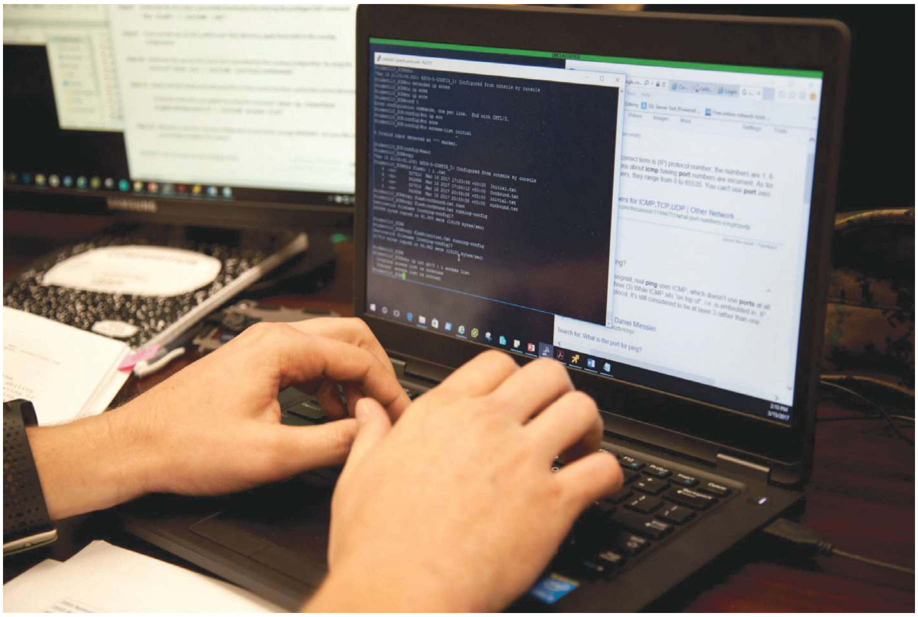
> Maybe there is an opportunity for us to look at other ways [of recruiting cyber forces], kind of the Marine Corps Band model where you bring in gifted musicians and you make them Staff Sergeants and then they spend their years in the White House in a red uniform, but they are Marines. So we are going to look at everything, we are going to look at all those models. [10]

The idea of allowing civilians to assume the title "Marine" based on their skill in the cybersecurity industry violates the foundation of what it means to be a Marine. From the very beginning Marines are indoctrinated with our institutional core values and dedication to the concept of mission and team over self. This invaluable and intangible quality distinguishes military service from many other professional models and is why qualified Marines are a valuable commodity in any workforce. Thankfully, the Marine Corps has not yet entertained this concept beyond casual conversation.

An alternative approach, mentioned by the former Commandant, Gen Robert B. Neller, is the adoption of the Assess and Select (A&S) model used by Marine Forces Special Operations Command (MARSOC).[11] This system allows Marines from any MOS to go through the assess and select process for potential entry into that elite group. Once a Marine enters the special operations community, they take on the MOS 037X and never return to the Fleet Marine Forces. Where this comparison breaks down is that MARSOC offers Marines the opportunity to be elite warriors who complete missions and gain combat experience they would not receive anywhere else. Should they leave that community, it is unlikely their special skills will seamlessly apply to another high-paying industry. In contrast, the eighteen-year-old Marine who takes on the 17XX MOS and gains advanced training and technical experience will quickly realize that he or she is not doing the kinds of work pictured in recruiting commercials. Further, they can do essentially the same job from a different cubicle in private industry or Federal service for significantly more money and with less encroachment on personal liberty. However, one useful comparison between the fields is that MARSOC operators earn over $10,000 per year in incentive, special duty, and hazard pay, which is based on compensation for low-density skills and not inclusive of retention bonuses. Similar compensation should be considered for the kinds of skills the force requires of Marines conducting cyber operations.

Marines from any MOS could go through an assessment process and become a member of the cyber community. *(Photo by Cpl Victoria Decker.)*

Because training a cyber warfare specialist requires years of costly training and experience, the Marine Corps should consider a human resource model similar to its aviation community. In exchange for incentive pay and valuable training, Marines would be required to sign extended commitments and demonstrate performance under pressure, allowing the service to build a highly-trained yet sustainable cyber workforce primarily comprised of uniformed members. Marines operating in the cyber domain would slowly gain both the certificates and experience necessary for employment in the industry as benefits of their service, while providing critical skills at great savings to the government compared to hiring Federal employees for the same job. To enter the 17XX cyber warfare field, Marines would agree to a six-year enlistment, starting after completion of approximately two years of rigorous cyber training. It is important to remember that the CMF's mission is to counter state-sponsored adversaries, or the foreign equivalent of NSA, which it cannot do with people who fail to meet requirements in a training setting. Should Marines fail to pass cyber training, they would transition to the communications or intelligence communities with a standard enlistment term. Under the plan outlined above, a Marine who has received the training and experience needed to be successful outside the military would first be eligible for exit from service eight years into his career. At this point, the roughly 26-year-old Marine should be offered another six-year enlistment that sends them to another round of advanced training, the start of a significant "cyber pay" annual incentive to close the wage gap with GS employees, and an additional retention bonus commensurate with the Corps' needs that year. Upon the completion of this enlistment they would be at 14 years of service and now practicing at the level of a master of their craft. At this point, having gained significant training and experience, many Marines are likely to exit service for much higher paying jobs elsewhere. Those who stay are the dedicated few who want to shepherd



Creating a cyber warfare MOS was the first step toward building a credible cyber force. ***(Photo by LCpl Jose VillalobosRocha.)***

the next generation or continue in a niche field like offensive cyber operations, neither of whom find greater income potential compelling enough to leave. A more effective incentive for these Marines may be the opportunity to remain in a geographic location, so long as there is an open billet, until they desire to move or choose to retire. Similarly, 17XX manpower models should consider allowing an E-7 to turn down promotion in favor of continuing to practice as a technician, thereby avoiding a promotion that would force them into an administrative role for the rest of their career. While the details and numbers of this plan are flexible, the tenets of extended time commitments and roughly equal compensation with the civilians who do the same job are critical to fielding a credible uniformed force in the cyber domain. Even after the significant annual "cyber pay" starting after year six, the government will have saved approximately $108,000 over the course of the Marine's career compared to hiring a federal civilian, with the added benefit of more predictable staffing across the force. To be sure, there is more to being a Marine than pay, but it is not an insignificant consideration as members venture into life events like home ownership and children. Until action is taken, the Service is accepting a natural limit to the expertise it is likely to achieve in uniform.

The Marine Corps cannot hope to outpace nation-state threats without the expertise of the field's best and most capable operators. The creation of a cyber warfare MOS was a necessary first step in the effort to build a capable cyber force and is helping to properly train, billet, and focus retention efforts. On its own, however, the specialized MOS only makes retention more difficult by ensuring that Marines are highly trained and provided advanced experience over a short period of time, especially early in their careers. The calling of a Marine is far more demanding than a typical job and should never be compromised. However, just as the service rewards special operators and aviators according to the demand of their skills, Marines practicing cyber operations should receive extrinsic benefits equitable to their civilian counterparts. If there is no change, Marines have few incentives, apart from a love of the Corps, to remain in cyber warfare billets, and it is unlikely that those who stay will be numerous enough to field a uniformly capable cyber force. The cyberspace domain offers many opportunities for advantage in future conflict, many of which the Marine Corps will be forced to neglect without taking aggressive measures to retain its well-qualified Marines.

Notes

1. Jim Sciutto, "OPM Government Data Breach Impacted 21.5 Million," *CNN*, (2015), available at https://www.cnn.com; Reuters in Washington, "US Military's Joint Staff Hacked as Officials Point the Finger at Russia," *The Guardian*, (August 2015), available at https://www.theguardian.com; and Hayley Richardson, "Companies Must See Cyber Attacks as Inevitable," *Newsweek*, (February 2015), https://www.newsweek.com.

2. U.S. Cyber Command Combined Action Group, "Beyond the Build," *Joint Force Quarterly*, (Washington, DC: National Defense University Press, 1st Qtr 2016).

3. Department of Defense, *Department of Defense Cyberspace Workforce Strategy*, (Washington, DC: December 2013); and Department of Defense, *2018 DoD Cyber Strategy and Cyber Posture Review,* (Washington, DC: 2018).

4. Gen David H. Berger, *38th Commandants Planning Guidance*, (Washington, DC: HQMC, 2019).

5. Kenneth Corbin, "Cybersecurity Pros in High Demand, Highly Paid and Highly Selective," *CSO*, (August 2013), available at https://www.cso.com.au.

6. Office of Personnel Management, "Salary Tables," (2019), available at https://www.opm.gov; further information available at https://www.opm.gov.

7. Information available at https://www.dfas.mil.

8. Evan Vucci, "Ashton Carter Considers Easing of Enlistment Standards," *NBC News*, (March 2015), https://www.nbcnews.com.

9. Jeff Schogol, "Every Marine A Rifleman No More?," *Marine Corps Times*, (May 2017), available at https://www.marinecorpstimes.com; and "Cyber Operations; Sea Services Panel," (panel, Navy League Sea, Air, and Space Exposition Day, National Harbor, MD, April 2017).

10. "Cyber Operations; Sea Services Panel."

11. "Every Marine A Rifleman No More?"

Command and Control Considerations for EABO

Marine Corps integration into the fleet via the Composite Warfare Commander concept

by Marc Riccio & Maj William Grimball

No single activity in war is more important than command and control. Done well command and control adds to our strength. Done poorly, it invites disaster, even against a weaker enemy.

—MCDP 6, Command and Control

As we continue to experiment with and advance the warfighting concepts outlined in the *38th Commandant's Planning Guidance,* it is not too early to begin the discussion of what the command and control (C2) structure for that envisioned force and associated missions might look like. Why is this even a concern? What is new? What is different about this new orientation that would warrant a legitimate look at C2 structures? The Commandant's words in his CPG may shed some light:

> Marines will focus on exploiting positional advantage and defending key maritime terrain that enables persistent sea control and denial operations forward.[1]

Gen Berger went even further in a recent speech at the Marine Corps Association Foundation Ground Dinner on 21 November 2019 in describing what this force would be capable of executing:

> our ability to conduct sea control and sea denial operations both from sea and from key maritime terrain is an essential naval capability in modern armed conflict … it is not a nice to have, it is essential."[2]

He further elaborated that

> those mobile, bad attitude, tool-kit packing Marines are focused on a small set of tasks to achieve sea control and sea denial; sinking ships, shooting down planes, killing enemy forces inside the area, and stopping all force from coming in."[3]

These roles are hugely different than the ones Marines have played in past operations involving the Navy-Marine Corps Team. For roughly the past 80 years, the Marine Corps has focused almost exclusively on the force projection ashore part of the naval mission of amphibious or expeditionary operations; the one exception being the introduction of defense battalions in the waning days before Pearl Harbor. How we got there was up to the Navy. Once we hit the high-water mark, we took it from there.

What has changed to precipitate this monumental shift? The obvious answer is that the threat has changed. The maritime terrain is once again relevant, particularly concerning potential adversaries and global peer competitors like China and Russia, and to a lesser extent Iran and North Korea. According to Gen Berger,

> China's pivot to the sea as the primary front in a renewed great power competition has fundamentally transformed the operational environment in which the Naval and Joint Force must operate.[4]

The U.S. Navy no longer possesses unchallenged global maritime dominance. Presumptive sea control is a

>Mr. Riccio is the Regional Director, MCU/CDET, Camp Lejeune, NC.

>>Maj Grimball currently serves as the Regional Chief Instructor of the Expeditionary Warfare School Blended Seminar Program (EWSBSP) for Camp Lejeune, NC.

Specifically, the Navy and Marine Corps must confront the new reality that presumptive sea control is no longer assured for the United States—we will compete for it.

—Gen David H. Berger

thing of the past. Our days of unchallenged sea control and sea denial have evaporated. Global competitors are actively and aggressively challenging that dominance. The range, volume, and sophistication of adversary anti-access and area-denial weapons make large maritime formations and fixed installations highly vulnerable and susceptible targets. Consequently, the Navy now embraces concepts such as distributed maritime operations and distributed lethality thru an integrated maritime defense. The Marine Corps' new role in supporting the maritime commander in this evolving and dangerous threat environment is captured in the *Expeditionary Advance Base Operations* (EABO) concept and the *deterrence* by *denial* strategy of the contact layer and the stand-in-forces.

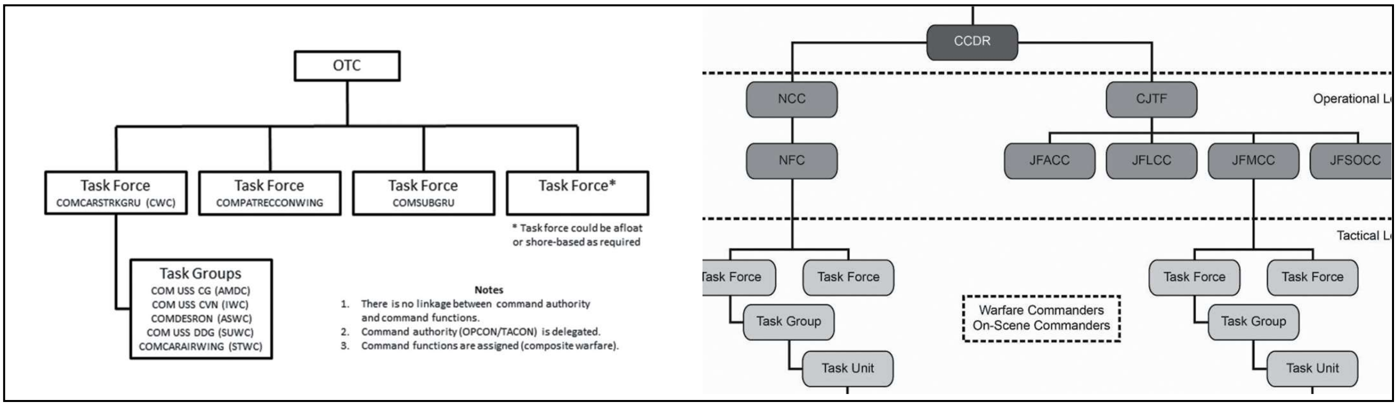
The key change is undeniable. The Marine Corps is no longer "along for the ride" and we recognize that we must play a more significant role in supporting the maritime commander's *sea control* and *sea denial* missions. If we are going to play an active role in maritime missions, we need to understand how these naval forces (specifically expeditionary advanced bases) integrate into and are part of the overall maritime C2 structure. To achieve this understanding, the naval force must address several fundamental questions. First, *what is the envisioned role of EAB forces in the sea denial and sea control missions as well as their role in the greater deterrence by denial strategy*? Secondly, *how are they integrated into the tactical naval architecture represented by the composite warfare commander (CWC) construct*? Thirdly, *who does the EAB force work for and what is the best organization and C2 structure to optimize the EAB forces contribution to the maritime fight*?

Addressing the first question, as described in the concepts of *Littoral Operations in a Contested Environment* and EABO, the Marine Corps seeks to further distribute lethality by providing land-based options for increasing the number of sensors and shooters beyond the upper limit imposed by the number of seagoing platforms available. Some examples of capabilities that might be provided by EABO forces includes intelligence, surveillance, and reconnaissance, coastal defense cruise missiles, anti-air missiles, forward arming and refueling of aircraft, and munitions reloading for ships and submarines. They may also control—or at least outpost—key maritime terrain to improve the security of sea lines of communications and chokepoints, or deny their use to the enemy, and exploit and enhance the natural barriers formed by island chains.[5] As such, these capabilities serve to increase friendly capacity and survivability while complicating adversary targeting inside the weapons engagement zone.

The terms* stand-in forces *and* inside-forces *are prominent in any discussion or recent literature on EABO.

The terms *stand-in forces* and *inside-forces* are prominent in any discussion or recent literature on EABO. Mr. Art Corbett describes in his February 2019 *Marine Corps Gazette* article, "Stand-In Forces: Disrupting the current struggle for dominance," that stand-in forces are forces with disruptive new tactical capabilities (several listed above) that will persist and operate forward within an adversary's weapons engagement zone. During day-to-day competition, stand-in forces enable the United States and our partners to confront *fait accompli* gambits and malign behavior with proportionate, responsive, and credible military options to match adversary aggression with commensurate force and risk. We are in affect deterring by denial through posturing forces and resources to detect aggression quickly enough to do something about it.[6] During conflict, stand-in forces may be employed as one of several simultaneous operational efforts within a larger joint campaign to defeat the counter-intervention strategy of peer adversaries.[7] In essence, EAB

Deputy JFMCC, BGen Chris Owens' flag flies over the JFMCC flag ship, USS* Mount Whitney *(LCC 20) during COMEUCOM Exercise* Austere Challenge *2009. (Photo courtesy of M.F. Riccio).



* Task force could be afloat or shore-based as required

Notes

1. There is no linkage between command authority and command functions.
2. Command authority (OPCON/TACON) is delegated.
3. Command functions are assigned (composite warfare).

Figure 1. **NWP 3-56*, pages 19 and 21.)***

forces are by definition stand-in forces. To clarify even further the often interchangeable terminology, stand-in forces describes a force positioned and designed to deter an adversary *fait accompli,* while inside forces describes a force that is actively operating within range of adversary long-range fires if and when deterrence fails.

With a basic understanding of the Marine Corps' role, via EABO in maritime sea control and sea denial missions, let us now shift our attention to the second question: How will these EAB forces and stand-in forces be integrated into the naval architecture represented by the CWC construct? The Commandant states,

> As an organization statutorily designated for service with the Fleet during the prosecution of a naval campaign, the Marine Corps must be able to quickly and effectively integrate into the naval forces.[8]

The Commandant further directs the Marine Corps to prepare to operate within the CWC construct. So what is the Navy's composite warfare construct? According to the *NWP 3-56*, the composite warfare organization enables offensive and defensive combat operations against multiple targets and threats simultaneously.[9]

Flexibility of implementation, reinforced by clear guidance to subordinates and use of command by negation, are keys to decentralized control of the tactical force. The officer in tactical command (OTC), normally the naval force commander or joint force maritime component commander (JFMCC), may implement a composite warfare organization whenever and to whatever extent required, depending upon the composition and mission of the force and the capabilities of the adversary.[10] The OTC uses task organization to enable a more reasonable span of control and to provide a framework for future delegation of authority. Tactical-level commanders task-organize to achieve military objectives by organizing assigned forces into task forces, task groups, task units, or task elements. Task organization allows an operational commander to divide and organize subordinate forces as well as assign authority and responsivity to plan and execute based on mission, platform capability, geography, or a hybrid of the three to address other issues and challenges.[11] (See Figure 1.)

The basis for all command and control is the authority vested in a commander over subordinates.

—MCDP 6

Furthermore, *NWP 3-56* states in a maritime operation area that has multiple task forces operating within it, the common superior (OTC) will be the numbered fleet commander /JFMCC. Unless this commander assigns OTC command functions to one of the task force commanders, the command will simultaneously be an operational- and tactical-level command.[12]

So the question remains: How does the Marine Corps integrate into the fleet composite warfare construct as directed by the CPG?

To determine this, we must address our third and final question: Who does the EAB force work for and what is the best organization and C2 structure to optimize the EAB forces contribution to the maritime fight? As described by the Marine Corps Warfighting Lab-Futures Directorate, EABO espouses employing mobile, relatively low-cost capabilities in austere, temporary locations forward as integral elements of Fleet/JFMCC operations.[13]

By definition and purpose, these EAB's are inherently *maritime* in nature. Think of them as a land-based naval platform. As such, it makes sense that the EAB force would need to be tightly integrated into the naval force commander or JFMCC C2 structure just as any other at-sea or airborne platform would be. It also allows the EAB force to take advantage of the resources represented by the other warfare commanders in the naval force writ large with access to all other CWC capabilities.

If the above argument is accepted, then logically the answer to our question is the EAB force would work for the naval force commander (this could be a Navy officer or a Marine officer). What might that organization look like? One potential option, and the one we propose for further study, would be to

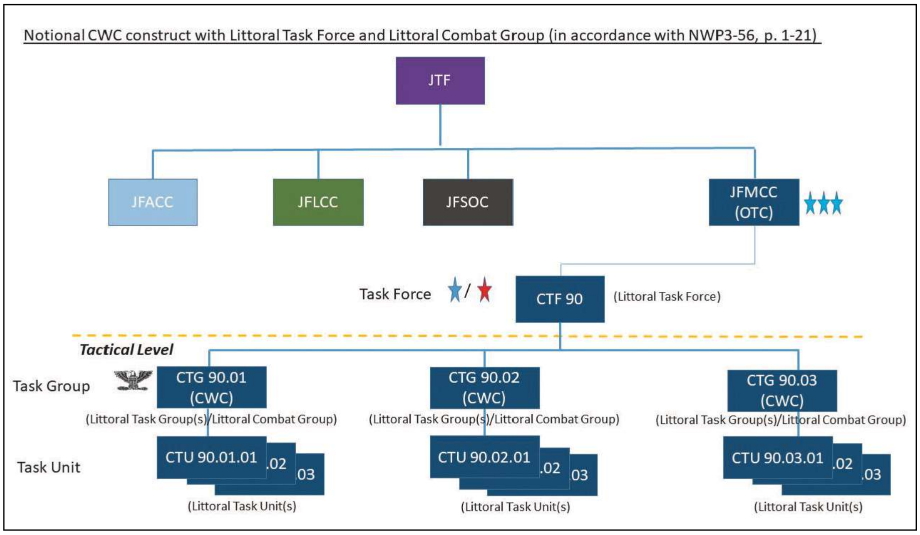


Figure 2.

develop under the numbered fleet commander/JFMCC, a littoral task force commander who would also be dual hatted as the littoral warfare commander for the Naval Force Commander/JFMCC. This commander would manage and control *all littoral operations* within a designated maritime area and inside the arc of enemy long-range fires. (See Figure 2.)

This designated littoral task force could be task organized with subordinate littoral combat groups (one or more) which would consist of afloat platforms and EAB forces. (See Figure 3.) Each of the LCGs would be assigned a specific area of operations that would or could include one or more EAB's. (See Figure 4 on next page.)

These "tool-kit packing" EABs of different sizes and capabilities would fall under the command authority (operational control) of the littoral combat group commander. In this way, the EAB would be tied directly into the CWC C2 structure overseeing all naval operations in the amphibious operations area. All collection, sensing, queuing, and shooting, both lethal and non-lethal, would be connected and coordinated by and through the littoral combat group. The EAB would indeed be an extension of the naval force commander. Although the systems that would allow this to happen have not yet been fully developed, the C2 structure that will best optimize our abilities and capabilities as an EAB force contributing to the sea control and sea denial missions should be discussed and discerned now in order to help decide these future technical requirements.

If we agree to the supposition that an EAB force is an extension of the naval force commander, a virtual ship on solid ground, and that these forces must be fully integrated into the CWC in support of the maritime missions of sea control and sea denial, then the next logical step is that these forces—regardless of whether they are operating as contact layer forces or blunt layer forces—work for the naval force commander (i.e., the littoral group commander in this proposed C2 structure).

Are we proposing to alter or change the time-tested commander amphibious task force/commander landing force command relationships? The short answer is no. If and when executing any of the five doctrinal amphibious operation missions, the commander amphibious task force/commander landing force, supporting/supported command relationship model is still sound. The proposed C2 structure and command relationships proposed in this article specifically address the Marine Corps' new role as an active participant in the maritime commander's sea control and sea denial efforts.

> ***... the C2 structure that will best optimize our abilities and capabilities as an EAB force contributing to the sea control and sea denial missions should be discussed and discerned now in order to help decide these future technical requirments.***

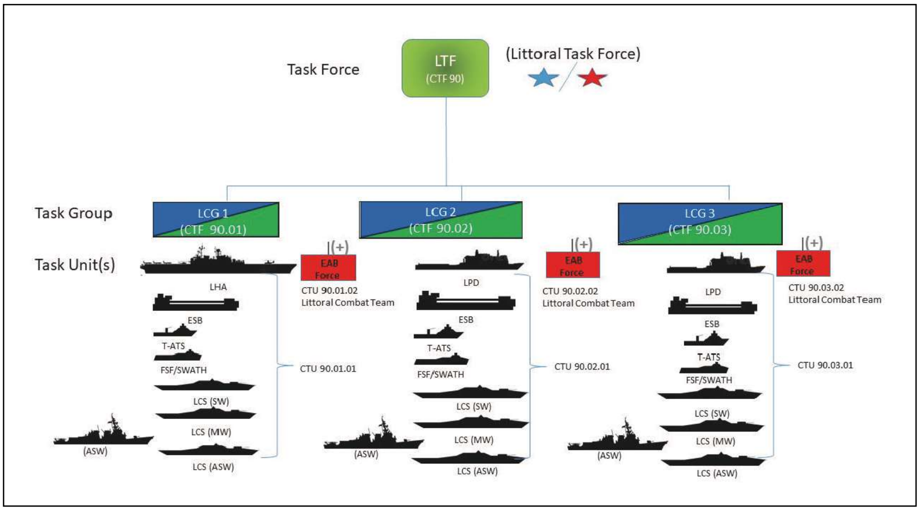


Figure 3.

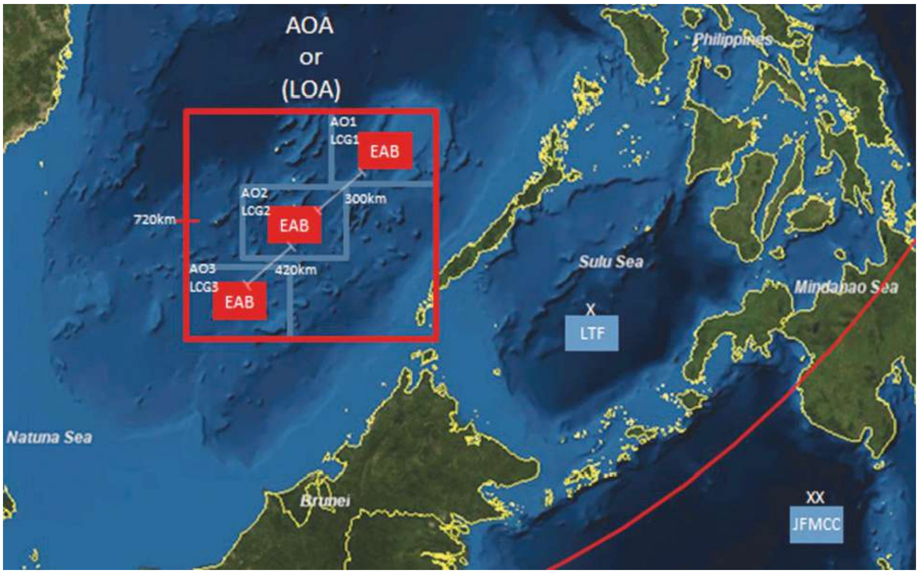


Figure 4.

Done well, command and control adds to our strength. *(Photo by Cpl Xavier McNeal.)*

We concur that Marine commanders are flexible and agile enough to adopt and operate within different C2 structures based on task organization and mission. If executing maritime missions in the littorals as an EAB force, the littoral task force/LCG command and control structure proposed in this article would be applied. If executing one of the five amphibious operations the commander amphibious task force/commander landing force model would be more appropriate.

In either case, it will do us well to remember, as stated in *MCDP 6*, "Done well, command and control adds to our strength. Done poorly, it invites disaster."[14] Let's not invite disaster. We encourage rigorous debate on this crucial topic, and we look forward to advancing the discussion.

Notes

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

[2] Todd South and Philip Athey, "We are the Front Line: How the Top Marine Wants the Corps Sinking Ships, Shooting Down Planes, and Killing Enemy Forces," *Marine Corps Times*, (Springfield, VA: November 2019).

[3] Ibid.

[4] Gen David H. Berger, "Remarks at the MCAF Ground Dinner," (remarks, MCAF Ground Dinner, Arlington, VA, November 2019).

[5] Marine Corps Warfighting Laboratory, *Concepts and Programs*, (undated), available at https://www.candp.marines.mil.

[6] Mike Gallaher, "State of (Deterrence) Denial," *The Washington Quarterly*, (Washington, DC: Elliot School of International Affairs, Summer 2019).

[7] Col Art Corbett, USMC(Ret), "Stand-in Forces," *Marine Corps Gazette*, (Quantico, VA: February 2019).

[8] *Commandant's Planning Guidance*.

[9] Department of the Navy, *NMWP 3-56, Composite Warfare: Maritime Operations at the Tactical Level of War*, (Washington, DC: December 2015).

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] *Concepts and Programs*.

[14] Headquarters Marine Corps, *MCDP 6, Command and Control*, (Washington, DC: 1997).

The Expeditionary Communicator

The naval C4 integration imperative

by CWO3 Emedin Rivera & Capt Ian P. Paquette

>CWO3 Rivera is the Space and Waveform Integration Officer, Systems Planning and Engineering, G-6 1st Marine Division.

>>Capt Paquette is Cyber Network Operations Officer, Information Environment Division, Fleet Marine Forces Pacific.

In a Congressional hearing during spring of 2012 Gen James F. Amos told congress, "The Marine Corps is not designed to be a second land army," regardless of our success in Iraq and Afghanistan, he said the Corps "is designed to project power ashore from the sea." With the Corps' shift back to its amphibious roots, the Marine communicator faces a significant deficiency in the understanding of amphibious doctrine, blue-green system integration, and expeditionary communications. For nearly two decades, a generation of Marines have "relieved in place transfer of authority" between forward operating bases at a cyclic rate to existing infrastructure and settled into firm bases with objectives to maintain and optimize existing tactical networks. Moreover, the reliance on heavy civilian contractor support exponentially grew over this time because of a technically deficient qualified force. The expeditionary communicator skills have atrophied in this environment. The Marine communicator has an entry-level basic training curriculum focused on specific systems and very little time is spent on theories and employment concepts. System specific operator training is inefficient. In particular, training does not include theories and principles of amphibious communication.

A Vision for the Future Force

In March 2014, Gen Amos laid out a new vision for the Corps through a document called *Expeditionary Force 21*. In the document, he recognized the need for the Marine Corps to restructure and refit to remain a force that is true to its amphibious roots. The Marine Corps' unique capability of immediate power projection coupled with credible decisive action against our Nation's foes makes our Service an indispensable tool for the President and is a peace of mind to the American people. However, the complexity, speed, and dispersed nature of current and future operations in the maritime environment will make command, control, communication, and computers (C4) a challenging arena. Our ability to gather, process, protect, and distribute actionable information to warfighting agencies at near realtime speeds will determine our effectiveness in the fight to come.

In September 2016, Gen Robert B. Neller revised *Expeditionary Force 21* and republished a new document titled the *Marine Corps Operating Concept*. In it, our 37th Commandant identified five critical tasks vital to shaping a viable, relevant, and lethal future force. The first critical task listed was "Integrate the Naval Force to Fight at and From the Sea." The inherent and unique challenges of Marines operating from the sea are consistently evident in today's force. Flag-level amphibious objective exercises like BOLD ALLIGATOR, DAWN BLITZ, and SSANG YONG all revealed comparable gaps between "fighting tonight" and the realistic lead times necessary to prepare integrated, responsive, and resilient networks suitable for a joint or combined maritime force. The bureaucratic processes required to enable networks for effective maritime operations on board naval assets does not support the "fight tonight" concept of employment. Agencies like Pacific Regional Network Operations Center, Regional Satellite Support Centers, Defense Information Systems Agency, Space and Naval Information Warfare Systems Command (NAVWARSYSCOM), United States Forces Korea, and Marine Corps Cyber Operations Group, among others, are not synchronized and all have lengthy procedural requirements that must be completed in order to enable capability to the commander of the landing force. The current status quo is not conductive to a force that prides themselves in readiness. In 2019, our 38th Commandant, Gen David H. Berger, published his guidance to the force. In it, he committed to fundamentally redesigning our Corps into a truly integrated naval force. The 06XX community is a key enabler of our force redesign.

An Expeditionary Training Imperative

Before 11 September 2001, our deployment cycle centered training on being expeditionary. We trained to embark on a ship, communicate from the ship, go ashore, and communicate ashore in a seamless transition that was transparent to command and control (C2). Fast forward two decades later and the 06XX community of today has morphed into something that looks closer to Army signal units than Marine units of old. Marines are expected to be naval in character and capable of conducting C4 amphibious operations in the high seas, the littorals, and ashore. However, the C4 community is simply not ready. There are zero formal learning centers that effectively address the 06XX communities' amphibious deficiency; neither the Marine Corps Communications Electronic School, Communications Training Center, nor Expeditionary Warfare Training Group Pacific/Atlantic deliver meaningful solutions. A deficiently trained force is compounded by a substantial blue-green system integration problem. The amphibious naval fleet is a cryptic collection of C4 systems that do not readily integrate with combined, joint, or organic Marine systems.

Expeditionary Force 21 presents an array of concepts that help illustrate the need for the 06XX community to realign inside expeditionary concepts. The expectation that Marine communicators are going to be able to reliably standup complex satellite and terrestrial networks fully integrated into existing data networks supporting enterprise services while embarked on naval vessels has always been there. However, the reality is that the population of proficient expeditionary communicators is small in proportion to the total force. The following are some excerpts from *Expeditionary Force 21* that directly address networks and systems:

> Ability to send limited data via a terrestrial communications system or systems with a 65 nm minimum range via line of sight, retransmission, relay, or combinations of all three means.
>
> Providing landing forces and support craft with beyond-line-of-sight, over-the-horizon, and on-the-move C2 systems capable of operating in a satellite-degraded communications environment.[1]

Many of the C4 concepts, equipment employment, and doctrinal principles presented at a MEU are not present in many other communications units throughout the Corps. Entry- and career-level formal learning centers throughout the Marine Corps do not present practical C4 solutions for amphibious operations. The Marine Corps Communications Electronic School does not offer meaningful C4 amphibious doctrine or systems integration courses. The Communications Training Center is an equipment-centric learning center that does not apply any amphibious concepts in their curriculum. The 06XX community at Expeditionary Warfare Training Group Pacific/Atlantic over the years have been reduced to support staff that seldom trains Marines on expeditionary communications. EWTGs have no formal programs of instructions on expeditionary communications. For these reasons, Marines attached to MEUs are seldom ready to deploy as effective expeditionary communicators. The learning curve is steep for many young and mid-career Marines who are faced with a landing force operations center or a supporting arms coordination center for the first time and do not know where to begin. Many are exposed to blue-green integration concepts for the first time during MEU/ARG composite unit training exercises just months before deployments. This usually generates command relationships that slow integration, responsiveness, and increase cultural misunderstandings.

... include requirements for a baseline understanding of amphibious communications ...

The 06XX community would benefit from re-evaluating the process of how it prepares Marines to enable C4 from amphibious ships. Marines who have the resident skill necessary to be effective enablers onboard our amphibious fleet are scarce. Liaison Marines attached to expeditionary strike groups are uniquely conditioned to be proficient in an amphibious environment. However, more needs to be done at the Service level.

In the last version of the training and readiness manual, there was only two requirements for C4 amphibious operation competency. These prerequisites were the only formal school-house requirements published. The word amphibious comes up four times in the document. Two events are communications officer requirements and two are in the title of referenced publications. Nothing is mentioned about operator requirements in amphibious operations:

- Develop an MSE level communications plan (0603-PLAN-2001).[2]
- Develop an MSC/MAGTF communications plan (0603-PLAN-2001).[3]

The training and readiness program should include requirements for a baseline understanding of amphibious communications (indoctrination) on board amphibious ships. Our training continuum should reflect a building block approach that accounts for the inherent complexity of amphibious communications: specifically, Navy programs of record in support of Marine Corps operations and familiarization of landing force operation centers onboard amphibious ships. The EWTGs are uniquely in position to provide the type of amphibious communications training that would make the community a more expeditionary force. The EWTG N36 section is staffed and equipped with Marines poised to instruct amphibious communications. A revitalized amphibious communications program that prepares the 06XX community to be effective enablers onboard our amphibious fleet is necessary as we pivot toward a more relevant maritime force.

The need for a tailor-made training and certification package for Marines joining or deploying on MEUs must be implemented. Most Marine units have grown accustomed to static C4 nodes in permissive environments. Installation of shipboard systems and the ability to effectively transport, distribute, and deliver information while embarked on amphibious ships are skillsets necessary across the force. A basic understanding of the capabilities and limitations of ship systems are voids that need to be addressed in a training environment, not off the coast of North Korea.

Enduring Frustrations at Sea, the Littoral, and Ashore

The trends are consistent. The lack of comprehensive C4 standardize amphibious training packages and poor blue-green system integration is obvious. The effectiveness and reliability of C4 during amphibious operations has been reliably inconsistent for many years. The following excerpts from past MEU deployments date back to 2011 but were sadly still relevant as recent as 2018:

> The lack of Marines cross-trained and capable of extending C2 across three ships, forward planners and MSE assets placed ashore threatened the accomplishment of MEU METLs. Organizing, training and equipping communication support teams to fulfill mission requirements was a priority during the first part of PTP. This delayed the training of other components of the MAGTF while critical skill sets were developed. The shortened PTP hindered integration and training of the MSEs negatively impacting training opportunities on combat operations center (COC) and the Command Post of the Future (CPOF) communications suite utilization.[4]

> One problem was supplying sufficient C2 manpower to make full use of the LPD C2 suite. On the Green Bay, the disaggregated ACE had to rely on the BLT's communications personnel for support. While the Green Bay possessed increased C2 capability, the older LSD (USS Comstock) lacked the capability for the Marines to effectively pass data without making use of Navy communication assets from time to time.[5]

> The 13th MEU communications section (S-6) had integration with the Navy aboard ship as its main priority during the PTP. With communications, no two Navy amphibious ships are structured the same and the MEU needed to understand its capabilities and limitations aboard ship. The MEU S-6 emphasized his dependence on the Navy while the MEU was on ship. He recommended any MEU S-6 visit and coordinate with his Navy counterpart as a first action.[6]

The *Marine Corps Operating Concept* reinforces the urgency for fundamental change in our training, task organization, and system integration. Nowhere is this more relevant than the way the Corps integrates with the amphibious naval fleet. Most units predominantly embark onboard amphibious ships weeks before an exercise and spend the first week trying to find the landing force operations center and mess decks. The learning curve is massive for the average communicator. Although MEUs fair a bit better, six or seven months of integration is still not enough:

> The Marine Corps is currently not organized, trained, and equipped to meet the demands of a future operating environment characterized by complex terrain, technology proliferation, information warfare, the need to shield and exploit signatures, and an increasingly non-permissive maritime domain.[7]

The Systems Integration Imperative

If the MAGTF is going to be an enduring, viable, and responsive maritime force at any level, it must develop C4 integration tactics, techniques, and procedures onboard amphibious ships that are more intensive and enduring than MEU composite unit training exercises or other integration exercises of short durations. A MAGTF that expects to come from the sea must create enduring and habitual practices at every level of the blue-green team that result in tangible enduring solutions to the landing force here and now.

The learning curve is massive for the average communicator.

Technical objective liaison teams that represent the interest of the MEFs should be staffed at the MEB/MEF level. They should imbed with ARGs and expeditionary strike groups with the prime objective to solve the inherent blue-green complexities of system integration on board amphibious ships. Moreover, the teams should focus on enduring relationships between the Navy and Marine Corps Team in order to facilitate collaboration and efficiency that could never be achieved in a two-week visit or even a six-month deployment. For instance:

> Communications and hence command and control were most difficult while on ship. Navy officers were surprised when I told them, 'When I get off this ship, I will have good communications.' We need to make our onship communications equal to those ashore.[8]

Achieving a well-qualified technical force is just as important as solving the challenges of blue-green system integration. Moreover, the transition of C4 nodes from ship-to-shore must be a prime essential task to our commanders.

I MEF's Dawn Blitz provided many lessons learned and was an overall success in 2015. However, a critical MEB command element capability was not completely flushed out during the exercise. The joint task force enabler detachment's ability to conduct a MEB command post exercise from ship-to-shore and validate C4 requirements for manning, organizing and training was not flexed. The logistical, wideband, and technical control challenges of transitioning a MEB command element ashore are still highly conceptual and are not clearly defined requirements in standard operating procedures or doctrine. The need to fully vet a truly amphibious MEB joint task force enabler capability cannot be replaced with transitioning the staff into the MEF Operations Centers or other controlled C4 facilities and exercise staff functions without validating the challenges of moving (ship-to-shore) key enablers and putting online a fully operationally capable tactical C4 node.

There are inherent integration problems with Navy and Marine Corps systems. The addition of a combined maritime force adds a layer of complexity that is yet to be clearly understood or articulated. The solution to partner interoperability must begin with joint force interoperability. C4 naval integration must serve as the principal and foundational objective for all other force integration.

Over the horizon and line-of-sight C2 must be improved for the landing force. ***(Photo by Cpl Nathan Reyes.)***

III MEF's SSANG YONG 2018 also revealed valuable lessons, most notably that system and network interoperability in combine operations does not support effective C2. The Combine Enterprise Regional Information Exchange Systems (CENTRIXS) Korea network onboard was not fully interoperable, which limited access to coalition C2 tools and impacted the responsiveness of the landing force. During the conduct of the exercise, it was evident that Navy and Marine Corps systems did not have the compatible versions of software or hardware needed to enable situational awareness, chat, and other collaboration tools. Moreover, the domain trusts necessary to enable single sign-on to information technology resources did not exist between participating commands. NAVWARSYSCOM's "Authority to Operate" directive and baseline ship restrictions aboard USS *Bonhomme Richard* and USS *Wasp* prohibited necessary modifications that would have facilitated deployed Marine domains aboard. The landing force was supplemented with Navy systems that allowed connections to CENTRIXS-K outside landing force operation centers. This solution was limited to a small number of users and was not ideal for collaboration. These—amongst a host of other systems integration issues—revealed that the blue-green team not only has to work better jointly but that coalition partners are far behind with systems that can integrate with Navy and Marine systems. In order to have combined collaborative information environments, we have to develop systems that integrate at the lowest common denominator.

The C4 community requires a fundamental shift in the way we enable C2. Marines must transition from a mindset of prolonged stationary comfort to an expeditionary one. What does a force conceived for the sea need to effectively C2 today? It needs to improve employment of over-the-horizon and line-of-sight systems in order to expand options and capabilities to the landing force. It needs to understand networked platforms and applications that expedite continuity of operations not delay it. It needs to improve its information processing capabilities and compatible C2 services in order to enhance amphibious operations, not detract from them. Most importantly, it needs to truly integrate blue-green systems by reducing like capabilities and streamlining collaborative systems.

The challenges encountered aboard amphibious ships today are unique to the ship. Specifically, *blue in support of green* systems that are managed by Navy personnel but operated by Marines. Enabling a commander's critical exchange information requirements are dependent on three domains: the transport (*connect*), network (*distribute*), and services domains (*deliver*). All three domains are not efficiently integrated onboard amphibious ships today. Every domain requires significant coordination to enable seamless ship-to-shore C2. The prevailing assumption is that the Navy provides the embarked force infrastructure to support Marine networks and domains. In reality, the entire system is Navy owned, accredited, and governed. It provides Marines little flexibility to support critical and unique *information exchanges requirements*. The afloat MAGTF C4 required capabilities letter produced by HQMC Combat Development & Integration identifies capabilities urgently needed onboard L-Class ships. However, if the fight is tonight, much urgent work is needed; we should adhere to the *Marine Corps Operating Concept*.

Transport

According to the MOC:

> Our ability to successfully execute the concept will depend greatly on the extent to which we have; overcome the enduring obstacles to leveraging and sustaining 'commercial-off-the-shelf systems'-because affordable '70%' solutions now are better than outdated solutions 10 years from now.[9]

The transport domain composed of space, terrestrial, and optical/wired transmission systems connect all information exchanges.

Embarked landing forces require the capability to connect point-to-point and point-to-multipoint nodes via line-of-sight, retransmission, relay, and beyond-line-of-sight systems. These capabilities must reliably enable C2 to the landing force whether ships are underway, in the littorals, or ashore. Ships are uniquely dependent on the electronic magnetic spectrum. The electromagnetic spectrum is the only transport available to ships. Therefore, compatible dynamic waveforms are critical for resilient electronic magnetic spectrum operations onboard naval vessels.

High performance waveform, advance networking wideband waveform, single channel ground air radio waveform, integrated waveform, net centric waveform, among other commonly used waveforms used by Marines, must be interoperable with blue systems. Today, they are not.

The enhanced man pack UHF terminal antenna is a prime beyond line-of-sight narrowband satellite communications voice/data capability used by the landing force. Unfortunately, it is not compatible with the ships channelization system. The demand assigned multiple access system on Navy platforms does not support integrated waveform today. IW is a key capability used by fast moving ashore nodes. This limitation restricts a large percentage of Marine Corps narrowband satellite communications users' ship-to-shore interoperability and must be prioritized for integration.

The Digital Wideband Transmission System is the current onboard solution for connecting nodes via wideband line-of-sight. However, it cannot relay signals to aerial platforms, and it is not compatible with ashore Marine systems. More capable omni-directional self-healing systems are available and can be installed today. These systems would significantly improve and rapidly deliver voice, video, and data services to and from disadvantage ashore nodes.

Super high frequency system integration has not been validated between blue-green systems. However, the Marine Corps' very small aperture terminal family of systems can connect to shipboard Navy multi-band terminal via modem to modem connections by utilizing X or Ka-band. Installation of master reference terminals would enable more efficient and survivable time division multiple access that would further enhance integration of the force. Blue-green super high frequency interoperability would enable dynamic homing options to L-Class ships from and to Marine nodes ashore, reducing the dependency on fix Gateway sites.

Extremely high frequency terminals connect critical services to afloat and ashore nodes using some of the most protected waveforms in DOD. Capabilities like "cross-link" and low data rate provide the commander global reach via low probability of interception-detection, and anti-scintillation communications links. Although these systems are blue-green compatible, the relationships needed to establish enduring connections as standard operating procedure do not exist. Today, the Marine Corps secure mobile anti-jam reliable tactical terminal can connect to the shipboard Navy multi-band terminal. However, it is never leveraged as an operational capability.

Networks

As stated in the MOC:

> Designed and protected our C2 and ISR [intelligence, surveillance, and reconnaissance] networks as a multi-source information sharing architecture that reliably serves disparate MAGTF elements—because distributing actionable information keeps operations in chaotic environments from becoming chaotic operations.[10]

The network domain composed of switches, routers, and boundary control devices distribute all information exchanges.

The Navy does not allow the embarked force to operate with organic Internet protocol space. Instead, Navy Internet protocol space is assigned to Marines while embarked, preventing seamless transition of C2 nodes from ship-to-shore. The local area network aboard a ship can be configured to support both Marine Corps enterprise networks and Navy enterprise domains simultaneously while maintaining cybersecurity standards. Naval vessels should reflect architectures identical to a small joint base, allowing multiple service enclaves distribution paths over shared infrastructure. On-board security stacks could facilitate inter-enclave connectivity while maintaining segmentation and security. Shared network infrastructure would enable a joint force on-demand access unclassified, classified and coalition networks. This flexible network capability would permit responsive distribution of information to mission dependent C2 requirements.

Deployed Marine forces and Navy ships utilize significantly different architectures in enabling wide area network connectivity. Network technologies like black-core routing and virtual routing forwarding are utilized both services; however, they are not interoperable. Ground units have long benefited from Defense Information Systems Network–Tactical Edge a global enterprise network allowing network connectivity of multiple enclaves. Defense Information Systems Network–Tactical Edge enables wide area network connectivity between tactical communications sites and enterprise entry points, enable the Fleet Marine Force flexible transport site options. Naval network architectures are proprietary networks that enable wide area network connectivity between deployed ships and ashore services. These significant variables in architectures hinder Marine and Naval communicators from enabling information exchange internally to the ship and external to enterprise entry points. Alignment of afloat and ashore network architectures is vital to FMF and Naval C2.

Services

According to the Marine Corps Strategy for Assured C2:

> The Marine Corps cannot meet the demands of the future warfighter with separate network designed for 'garrison' and 'deployed' operations. The need for greater mobility and rapid deployment render our current C2 construct grossly inadequate.[11]

The services domain composed of directory services, unified communications, information assurance, and C2 applications deliver the commander's critical information.

The Deployed Marine Corps Enterprise Network (DMCEN) concept of employment provides a highly responsive network enabling staffs to respond to contingencies in compressed timelines. DMCEN delivers local services to forward deployed units regardless whether they are disconnected or disadvantage from the enterprise. Although the concept has been tested repeatedly, deployments of Marine Corps enterprise network services aboard naval vessels continues to be problematic. Programmatic and accreditation issues between Headquarters Marine Corps and NAVWARSYSCOM prevent the embarkation of DMCEN onto naval vessels without significant coordination and special arrangements. Although technically feasible today, FMF units require top down momentum in order to generate configurations for Consoidated Afloat Network & Enterprise Services that would allow for the deployment of MCEN services aboard naval vessels as a standard baseline and not a custom solution.

A digitally integrated joint force requires a large portfolio of C2 applications in order to execute operations. Navy and Marine programs of record require complex configurations and coordination in order to enable interoperability. Program of Record C2 application utilize custom, unfamiliar, Internet Protocol ports. To fully integrate the systems capabilities, firewalls and other security devices must be specifically configured on a per mission basis in order to enable information exchange. Change requests are required per respective network operating center, which neither efficient nor effective; troubleshooting of blocked ports is tedious and exacerbated by complex distribution networks. Due to highly customized features, C2 applications also utilizes a variety of message formats. Twenty-plus years of grounds based operations has resulted in Marine Corps C2 systems being more interoperable with Army systems then Navy systems. Standardization and documentation of IP ports and data messages will enable whitelisting of traffic and enable interoperability between systems. Other C2 services like unified communications, chat, and collaboration services should be engineered in combination with Joint Task Force or Combatant Command systems, one-off solutions that do not replicate or communicate with ashore command structure impairs the expeditionary communicators abilities. Blue-green system integration must be prioritized at every level of the decision cycle; the efficiency and lethally of the maritime force depends on it.

To improve our ability to fight at and from the sea, we must: Collaborate with Navy counterparts to establish austere, scalable, and agile EABs.

Conclusion

The Corps is relevant for its creed as much as its capabilities. The ethos its warriors practice is valued as much as the equipment they carry. Its commitment to a selfless and fearless culture keeps the force relevant. However, the Corps must fiercely align limited resources toward making Marines the undisputed force of choice for power projection from the sea. Proper training and system integration will uniquely enable the force. A middleweight and highly specialized force that delivers the combatant commander valuable decision space and viable options in compress timelines. The Marine Corps C4 training pipeline must become "bluer" with deliberate objectives to improve blue-green system and culture integration. All MAGTFs must become bluer at all levels by active system and culture integration of units like expeditionary strike groups and MEBs. Service-level agencies like Marine Corps' CD&I and Navy's NAVWARSYSCOM must also assimilate systems acquisition and program management efforts that enable a truly integrated naval force. The challenges that have plagued blue-green integration are decades old. Today, agencies must target technical engineering integration solutions as much as the latent bureaucratic dissonance of dispersed agencies producing stove-piped solutions for a naval force expected to fight as a team:

> Lying offshore, ready to act, the presence of ships and Marines sometimes means much more than just having air power or ship's fire, when it comes to deterring a crisis. And the ships and Marines may not have to do anything but lie offshore. It is hard to lie offshore with a C-141 or C-130 full of airborne troops.[13]

When Maj Earl "Pete" Ellis wrote "Advanced Base Operations in Micronesia" (1921), not one amphibious ship existed in Navy or Marine Corps inventories. Sailors and Marines did not have a clear plan on how to conduct amphibious operations. Since then, the Navy-Marine Corps Team has exponentially matured this capability to a globally reaching credible deterrent against our Nation's foes. The advent of technological advances must enhance what Ellis began and not detract from the scope of what is possible from a fully integrated amphibious naval force.

Notes

[1] Headquarters Marine Corps, *Expeditionary Force 21*, (Washington, DC: March 2014).

[2] Department of the Navy, *NAVMC 3500.56D, Communications*, (Washington, DC: November 2019).

[3] Ibid

[4] Marine Corps Center for Lessons Learned, "26th MEU Operations Lessons and Observations from the 26th MEU Deployment, August 2010–May 2011," (Quantico, VA: 2011).

[5] MCCLL, "13th MEU: Lessons and Observations from 13th MEU Deployment, February-September 2011," (Quantico, VA: 2011).

[6] Ibid.

[7] Headquarters Marine Corps, *Marine Corps Operating Concept*, (Washington, DC: September 2016).

[8] "13th MEU Lessons and Observations."

[9] MOC.

[10] Ibid.

[11] Department of the Navy, *Marine Corps Strategy for Assured C2*, (Washington, DC: HQMC, March 2017).

[12] MOC.

[13] Headquarters Marine Corps, *Expeditionary Force 21: Marine Expeditionary Brigade Concept of Operations,* (Washington, DC: July 2014).

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

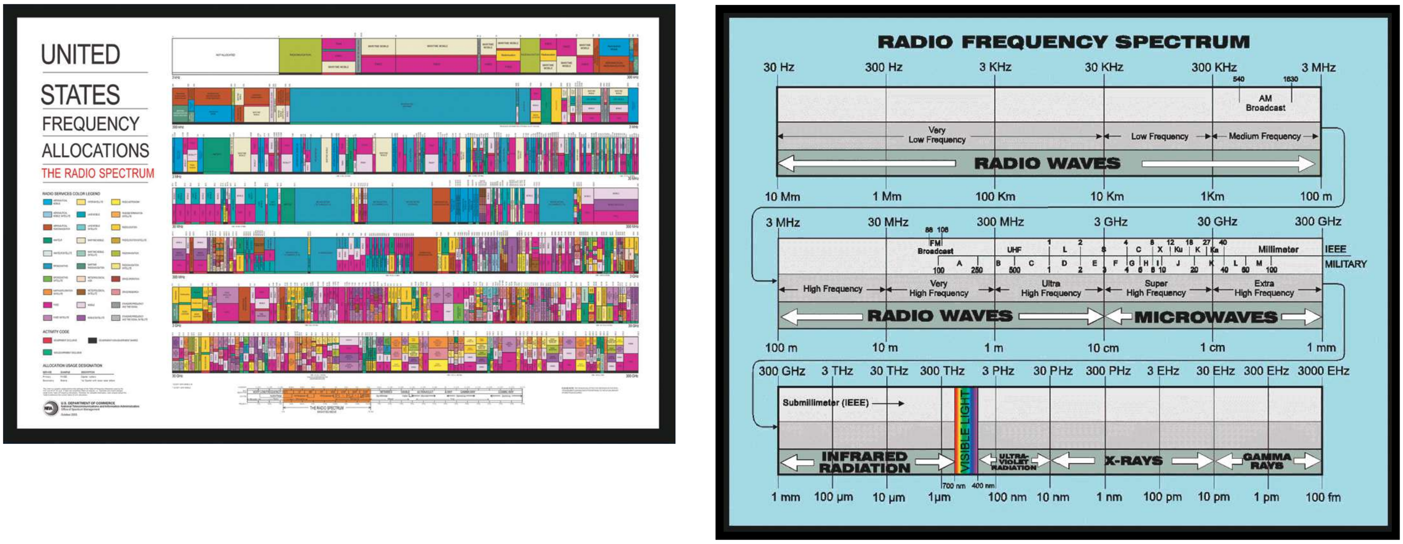


Figure 1. APPENDIX A: Frequency Spectrum Charts. The United States Frequency Allocation Chart. Source: U.S. Dept. of Commerce, National Telecommunications and Information Administration, Office of Spectrum Management, March 1996.

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

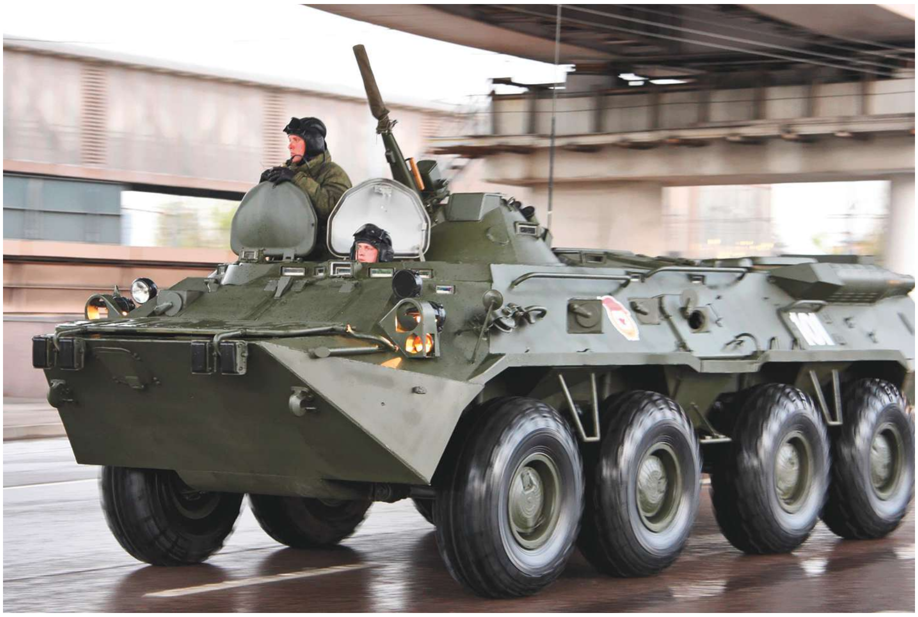


Figure 3. The Russian military has the capability to employ the BTR-80 with mounted jamming equipment. (Photo by Vitaly V. Kuzmin and is licensed under Creative Commons Atribution-ShareAlike 4.0 International license.)

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 multi-processor-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.

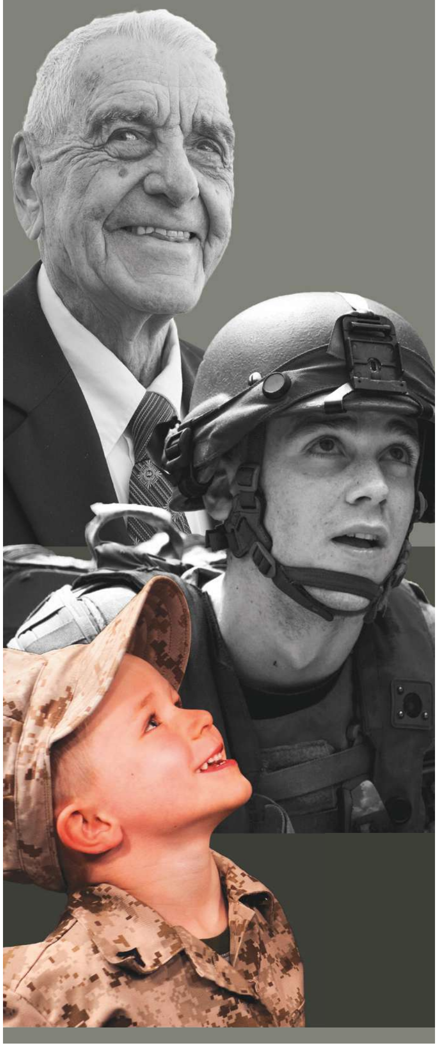
[37] IHS Jane's, "R-330T VHF Automated Jamming Station," (April 2016), available at https://janes-ihs-com.lomc.idm.oclc.org.

[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.*



ANW2 Expanded

Somewhere in South East Asia

by Maj Adrian E. Ybarra, 1stLts Raymond Ashton,
Ronnie Reyes, & Ryan McCoy

>Maj Ybarra is currently the Communications Officer, 11th Marine Regiment. He has also served as the Assistant Communications Officer, 15th MEU, and Communications Division Head, Marine Aviation Weapons and Tactics Squadron 1. He is also a graduate of the Joint C4 Planners Course and the Advanced Communications Officer Course.

>>1stLt Ashton is an 0602, currently serving as S6 Operations Officer, 11th Marines. He previously served as the Communications Officer, 1st Bn, 11th Marines.

>>>1stLt Reyes served as the Data Chief, Marine Corps Security Force Regiment, Team Leader for the MARCENT Commanding General's Communications Team, Alert Posture Force Officer in Charge, 4th Joint Communications Squadron, and is currently serving as the S6A for 11th Marine Regiment.

>>>>1stLt McCoy is a Communications Officer, 11th Marine Regiment.

The forward observer (FO) adjusted himself on the rocky ground as he observed an enemy emplacement through his optics. He witnessed large- and medium-sized vehicles, about twenty total, as well as many antennas satellite dishes all being packed up in a hurry. This was certainly a command and control (C2) node of some sort, and it would not be there for long. The enemy was definitely getting ready to displace. The battalion landing team (BLT) had established a foothold upon landing in the area of operations but had stalled in its advance inland. The opposition consisted of a highly motivated and capable fighting force with one apparent weakness: its reliance on centralized control. Early on, the enemy proved to be ever elusive, evading contact and being targeted by fire support by quickly disappearing with their ambush-and-evade tactics, but now their entire combat operations center (COC) was directly in front of him. Here in his reticle pattern was the enemy's Achilles' heel, an opportunity that had to be seized upon. Adding to the pressure, the enemy had tucked their COC in the middle of a local village.

Without delay, the FO began to generate the fire mission. This was the perfect situation calling for an, "At My Command," High Explosive/Precision Guidance Kit (HE/PGK) mission—a can't miss opportunity. He grabbed his FO suite and sent a message to his battalion fire support coordination center (FSCC). The BLT's fire support coordination center would simultaneously check for any conflicts and approve the mission. Suddenly, as if Murphy was playing a cruel trick on him, the sounds of small arms and mortar fire came from the direction of the BLT's COC. Over the tactical net, SALUTE (size, activity, location, unit, time, equipment) reports started flooding the net with short choppy phrases like "small arms … incoming … mortar fire … squad element." Erratic gunfire was mixed in with each transmission.

Unbeknownst to the FO, the skirmish he just heard caused significant damage to some of the COC's communications equipment. The very small aperture terminal (VSAT) dish, the battalion's primary data connection to higher and adjacent units, was destroyed and the networking on-the-move (NOTM) was knocked offline. The BLT had just lost all data connections via satellite assets.

The FSCC raised the FO on the conduct of fires net to tell him what had occurred with instructions to send a voice mission. Sure, the voice mission was going to take longer, increase the potential for error, and potentially preclude the use of precision munitions, but that was better than watching the target drive away. As the FO began preparing the voice fire mission, his digital suite made a little beep. Perplexed, the FO looked at the screen. A pop-up message displayed, "MTO: AD3074, F, 2, HE/PGK, AMC, MO 4251." As the FO was about to grab the conduct of fires net to find out what was going on, the FSCC came over and said, "We're still up digital with everyone." Another pop-up appeared, "AD3074, Ready." How was this happening? The BLT had lost all satellite equipment, but somehow the critical digital traffic was getting through. Not caring to ponder how the network was working but rather content in the fact that it was, the FO hit the "Fire" button.

A few seconds later in the Fox Battery position, six howitzers digitally received the command to fire over their section's chief display shortly followed by the thunder of their discharge. The FO received "Shot" and "Splash" messages right in time to bring his binos to bear on the target. In near unison, six rounds dissected the rectangular target without warning—courtesy of the fuse's precision guidance; twenty seconds later the final volley impacts, dashing the enemy's hope of delaying

FOs observed the impact of artillery rounds to determine need for a repeat fire mission. *(Photo by Cpl William Perkins.)*

the BLT's offensive. The FO scans the target, trying to decide if a repeat mission is necessary. There is no need; one of the line companies is maneuvering toward the position and will easily clear it. The FO taps "EOM" (end of mission); kilometers away, the howitzers traverse back onto their priority target.

Our FO was the beneficiary of a properly designed and configured tactical data network. Able to converge quickly, this network is rapidly adaptive, self-healing, and self-forming. Though the satellite access was eliminated by enemy action, the networking equipment was able to prioritize mission critical traffic and direct it over the tertiary line-of-sight networks populated by the PRC-117G and its variants. The network did this without end-user input, allowing the FO to focus on the critical tasks at hand. Meanwhile, behind the scenes, the network as a collective whole is constantly analyzing itself, ensuring reliable, adaptive, and timely transport of information. The waveform responsible for this is known as Adaptive networking wideband waveform (ANW2).

ANW2 has been in use in the Marine Corps for the past few years; however, its full capabilities have yet to be realized. 11th Marine Regiment, 1st MarDiv, Camp Pendleton, CA, was the first unit within the Marine Corps to transition from the Enhanced Position Location Reporting System (EPLRS) to the AN/PRC-117G/VRC-114 based ANW2 network as the primary backbone for digital fires. ANW2 has been in use throughout the Regiment for the past 30 months and has been fully integrated into the 11th Marines' communications architecture. Prior to the implementation of ANW2, the EPLRS system was never integrated into the full communications network; it was used as a separate system allowing the regiment to solely transmit digital fire missions. As the replacement for EPLRS, ANW2 has expanded the C2 capabilities of 11th Marines exponentially.

ANW2 is a self-forming and self-healing waveform for fixed and mobile tactical operations. It can ensure immediate and robust data and voice communications across the network while automatically detecting the path with the greatest data rate and use that as its primary avenue of transmission. Using dynamic discovery, should that avenue suffer from interference of any kind, ANW2 will automatically redirect its path to a different transmission source because the PRC-117G updates its routing paths every 30 seconds. As the network changes and radios move locations, the optimal data path is updated as well. Every radio within the ANW2 network acts as a repeater, and this has enabled 11th Marines to significantly expand the range of its transmissions and ability to C2.

The integration of ANW2 within the regiment allows for multiple digital communications paths to maintain C2 of subordinate units. The regiment hosts a 30 node ANW2 network that provides connectivity to each battalion's main and forward COCs as well as the counter-battery radar teams. Each battalion hosts its own 20 to 30 node ANW2 network extending connectivity to the battery level and to each maneuver unit's FSCC. The battalion clouds are routed to the regimental cloud using the network switch organic to the mobile tactical shelter. ANW2, used in conjunction with the VSAT/NOTM, creates a hybrid mesh network with multiple data paths available to each unit. The FSCCs, located with the maneuver unit each battalion is supporting, are integrated both with ANW2 as well as any VSAT or NOTM the unit provides. The ANW2 and satellite network integration creates an unprecedented level of communications between the infantry regiments and the artillery battalions in direct support. Each infantry regiment is tied directly to its supporting battalion's ANW2 network, enabling quick and efficient fires processing and data sharing while the redundancy provided by satellite communications allows for fires to continue if a unit is beyond line-of-sight (BLOS), a capability previously not available within the regiment.

With the full integration of ANW2, a data path is now available to the battery level, providing the primary means for digital fires throughout the regiment. In addition to digital fires, ANW2 has proven to be a viable solution to accessing other C2 applications without the use of wide-band satellite communications. The full mesh network extends secret Internet Protocol router (SIPR) services to the battery level in addition to Advanced Field Artillery Tactical Data System and digital voice communications. C2 applications such as chat, Voice over Secure Internet Protocol (VoSIP), command and control personal computer (C2PC), and web browsing are now available at the

The ANW2 has been in use for several years, but its full capabilities haven't been realized.
(Photo by Cpl Summer Romero.)

battery level. This has expanded the battalion's communications capabilities and enabled them and their batteries to pass digital information which was never previously available. Information such as imagery, digital files, position reports, fire capable reports, and the common operational picture can now be accessed quickly and securely.

The ability to extend SIPR network services throughout the regiment and down to the battery level has provided a reliable and redundant means to communicate without the use of wide-band satellite communications (SATCOM). SIPR, extended to the battery level through ANW2, allows the regiment to continue its operations in a SATCOM degraded environment. At the battalion level, the data paths have increased exponentially; for example, in the event a battalion NOTM becomes inoperable, network traffic can still traverse through the regimental ANW2 network and exit via the regiment's VSAT or adjacent through a sister battalion's NOTM. The mechanisms for this function are the Internet Protocol enabled switches present in each mobile tactical shelter. They perform the majority of routing for data traffic in the 11th Marines network. The switches choose the best path available for data traffic with ANW2 being prioritized because of its more specific route. In the event either pathway is lost, the switches will direct the data traffic through the next programed path. The failover takes effect automatically, is transparent to the user, and will revert back to the preferred ANW2 route when it is available.

The implementation and integration of ANW2 into the pre-existing network has dramatically increased capabilities but has also increased complexity. The addition of multiple data paths has increased the requirement for traffic management on an ever-changing dynamic network as the nodes update their routing table every 30 seconds. Traffic management has become more complex as multiple routing protocols are now being utilized simultaneously on one integrated network. Configuring the network has become a challenge as it well exceeds the entry school-level training of cyber network operators. 11th Marines has invested time and training into mitigating this issue by sending cyber network operators to commercial certification training, such as Cisco certified network associate and Cisco certified network professional courses. Without the knowledge base these certifications provide, the Marines would be unable to implement and maintain a network of this complexity.

Although great strides have been made in the employment of ANW2, more work needs to be done. 11th Marines is currently at work to extend ANW2 systems BLOS. They have successfully tested the broadband global area network (BGAN) terminal to bridge the ANW2 network BLOS. The developments have been significant for the HIMARS battalion as its batteries doctrinally operate BLOS from the battalion FDC. Additionally, the cannon battalions are expected to receive PRC-117Gs to replace the digital fire control system. The implementation of PRC-117Gs to the gun line will accelerate the kill chain, closing the sensor-to-shooter cycle for the warfighter. Any observer with digital connectivity will be able to send a fire mission directly to the gun line.

The impact that ANW2 has had on 11th Marines cannot be understated. By extending live SIPR services to the battery level and being able to tie maneuver units directly into its network, the regiment and its subordinate battalions have greatly enhanced their ability to C2 and provide precise and timely fires. Sharing information, passing digital fires, and communicating by voice have all been made easier with this waveform. The flexibility provided by merging ANW2 with the existing SATCOM network has created a redundant network for the 11th Marine regiment to communicate with its subordinate and adjacent units. This type of network can be scaled across the GCE and tailored to any mission and can provide critical data and communications means to the lowest level. While there are still improvements to be made, ANW2 provides a robust communications network that enhances a unit's ability to share information across the battlespace without the requirement for wideband satellite communications.

Wargaming

OIE practice reinforces OIE employment

by LtCol Dennis Katolin & Maj Benjamin George

The utility of wargaming is evident in the current Joint Strategic Planning System and the *38th Commandant's Planning Guidance*. The Joint Staff is wargaming to facilitate the future global integration of operations.[1] The Marine Corps is wargaming to support force design and to drive concept and technology development.[2] The human aspects of wargames also provide value by identifying the motivations, calculations, and consequences of a participant's decision making.[3] With the establishment of "information" as a warfighting function and the growing understanding of the consequences of the nature of the information environment, wargaming serves as a means for testing our application of operations in the information environment (OIE). Conceptually, OIE wargaming will provide a better understanding of how to exercise OIE functions to support operations across all domains.

Wargaming is part of a cycle of research that includes history, exercises, analysis, and current operations. Wargaming itself should not be confused with systems analysis or operations analysis; rather, it should serve as a method for identifying critical assumptions and related decisions and rationales.[4] As our understanding of the IE continues to develop, OIE wargaming allows us to identify critical assumptions about integrating the information warfighting function as a means of force preservation, power projection, and influence. Just as we test other warfighting functions for planning vulnerabilities—such as logistics sustainment or fire support—so too must we test our OIE functional plans to validate assumptions and identify our own gaps and limitations within the IE.

>LtCol Katolin is a Strategic Planner with Information Plans and Strategy Division, Deputy Commandant for Information. He twice deployed to Al Qaim, Iraq with 1st Battalion, 7th Marines and once to RCSW in Afghanistan with 9th Communications Battalion.

>>Maj George is a MAGTF Intelligence Officer with Information Plans and Strategy, Deputy Commandant for Information. He has deployed to RCSW in Afghanistan as an Intelligence Advisor to the Afghan Border Police and completed a WESTPAC deployment as the S-2A for the 11th MEU Command Element.

Challenges

There are a few challenges that make wargaming information difficult. The first is a lack of understanding of the IE. Information requires a new paradigm through which to conceptualize maneuver. Our information dependency exposes new potential vulnerabilities, while the nature of the IE extends our operational range and accelerates cause-and-effect relationships. There are several basic truths about the nature of information that can help us conceptualize the IE and identify how OIE can be wargamed.

Truth #1: Information is global, persistent, and immediate. The hyperconnected world allows information to cross the globe instantly, which makes the IE the most accelerated environment for military operations. The ability to project power and defend against the enemy's application of military power requires a global perspective with persistent presence and awareness.

Truth #2: Information requires convergence of maneuver across all domains. Traditional maneuver of forces through the air, land, and maritime domains has inherent informational impacts, while information itself can have significant effects in the air, on land, at sea, in space, and across cyberspace. Maximizing the utility of information requires the convergence of these impacts for an overwhelming effect on the adversary.

Truth #3: Military power is a combination of combat power and information power. Information and combat are mutually supporting and mutually enhancing. The relationship between them is so entwined that either can shift from main effort to supporting effort throughout the course of a single operation. Combat power has inherent impacts in the IE. Conversely, information power can amplify combat power by informing target audiences, influencing decision makers, and deceiving adversaries.

Truth #4: Information compresses the levels of war. Information is vital to tactics, campaigns, and strategies; it can impact everything from tactical formations to national institutions and globally networked communities. The immediacy and reach of information mean that tactical formations have potentially strategic impacts in the IE.

Truth #5: The information environment is maneuver space. Maneuver warfare is a philosophy that seeks to use a

> series of rapid, focused, and unexpected attacks designed to shatter the enemy's cohesion and create a situation with which he cannot cope.

There are avenues of approach in the IE through which we can project information and combat power to shatter the enemy's cohesion. The success of multi-domain maneuver is becoming more dependent on the execution of, and protection from, deliberate activities in the IE.

The second challenge to wargaming information is an incomplete understanding of the OIE functions and how they can be wargamed, which constrains our ability to effectively know *what* aspects of OIE should be stressed in wargaming. Similar to testing the functions of aviation or logistics, we must also stress our ability to perform OIE functions against a thinking adversary. (See Figure 1.)

Functions of OIE

1. **Assure Enterprise C2 and Critical Systems.**
2. **Provide IE Battlespace Awareness.**
3. **Attack and Exploit Networks, Systems, and Information.**
4. **Inform Domestic and International Audiences.**
5. **Influence Foreign Target Audiences.**
6. **Deceive Foreign Target Audiences.**
7. **Control Information Related Capabilities, Resources, and Activities.**

Figure 1.

A third challenge to wargaming information is the difficulty in translating qualitative data from human-focused functions into tangible results that impact game pieces on a map. Informational effects can be either quantitative or qualitative. Physics-based models have incorporated operations in the electromagnetic spectrum, cyberspace, and space into traditional wargaming methods because their immediate impacts are quantitative in nature. OIE functions with tangible effects on systems, signals, or access points can be abstracted to tokens and counters with quantitative data—number values and percentages—that can be employed and adjudicated within the parameters of the wargame. However, the effects of human-focused OIE functions that seek to inform, influence, or deceive audiences are based on human psychology, social dynamics, and cultural nuance—making them difficult to quantify and adjudicate. Percentages and number values do not easily translate to the human factors of war—atmospherics such as sympathy or distrust—and, as a result, they are omitted from the wargaming process.

Our tendency to focus on quantifiable data is purposeful; it is easier to assess, process, and predict results of quantifiable data, which ultimately supports capability and technological development. However, we must ensure that qualitative information effects are not overlooked. As *MCDP 1* states,

> any doctrine which attempts to reduce warfare to ratios of forces, weapons, and equipment neglects the impact of the human will on the conduct of war and is therefore inherently flawed.[5]

There is much to be gained from wargaming human-focused OIE functions. While we should strive to eliminate as much uncertainty as possible, Marines must become comfortable with the uncertainty of qualitative effects. Identifying assumptions and decision-making criteria for when and how to employ these OIE functions can support integration of the information warfighting function and develop proficiency and understanding for how to conduct OIE.

A New Model

The following techniques provide approaches for wargaming qualitative effects of OIE functions:

Function #5: Influence foreign target audiences. This function is critical to building and maintaining regional and global popular support. Units such as civil affairs and communications strategy companies can increase the Marine Corps' ability to gain access to critical host-nation infrastructure for sustainment, transportation, intelligence, and C2. Competitors and adversaries will compete for that influence, which will impact our operations. Previous wargames operated under the invalid assumptions that we were successful in out cycling our adversaries to gain needed influence. The following technique is a recommendation for challenging those assumptions to reinforce that we must compete for that influence.

Wargaming technique:

- Each side will identify objectives that they can achieve through influence; this can be access to bases, ports, airfields, or inclusion of military capabilities and forces. Both sides will focus influence in two areas:
  - The first area will be local populations and governments (which impacts access to infrastructure, resources, etc.).
  - The second area is global populations and governments (which impacts economic sanctions, inclusion of coalition forces, etc.). The process would work as follows:
    - Step 1: Influence objective. identify influence objectives and intended operational/tactical results (e.g., influence provincial leadership to gain port and base access to build combat power and deploy ships).
    - Step 2: Influence maneuver. Roll dice to adjudicate competition between blue and red players for regional influence. Advantage is given to the player who employs more influence forces (military information support operation teams, civil affairs, etc.). Each time a player wins an influence engagement, they receive an influence token. Influence tokens represent the "build up" of influence that, when aggregated, will reach a decision threshold for political leadership to react to, which will impact operational actions.
      -2 X influence tokens = a regional gain.
      -4 X influence tokens = a global gain.
    - Step 3: Influence impacts. The aggregate effect of winning an influence engagement must

result in decisions that impact operational or tactical maneuver elements (e.g., enough regional influence means denial of enemy access to infrastructure; enough global influence and we compel enemy's political leadership or an enemy's ally to restrict maneuver of their ground forces – similar to how political leadership called off Marines during the assault through Fallujah in April 2004). A regional/global gain can be played to either gain friendly access or deny enemy access.

Functions #1 and #3: Assure friendly C2 and attack enemy networks. Aspects of these functions exist in current wargaming, but the scope and scale can be expanded. There are now dedicated maneuver elements that engage each other constantly in the IE in execution of these OIE functions. The results have impacts across all warfighting functions. The global reach of cyberspace must compel commanders to think globally to determine areas of influence and interest and to identify potential targets within the IE. The following technique offers a construct to do so:

Wargaming technique:

- Step 1. C2 targeting. Each side must identify critical C2 nodes for both military organizations and national-level civilian infrastructure, similar to how we identify air fields on a map. Anything identified outside of the geographic combatant commander area of responsibility should be labeled on a piece of paper and attached to the map (e.g., servers for military logistics services for an enemy force located in a different continent).
- Step 2. C2 maneuver. Identify maneuver elements that can either strike or defend C2 systems. Dedicated tokens for offensive and defensive cyber organizations should be placed on the map to help identify capacity and likelihood of successful maneuver in the IE.
- Step 3. Adjudication. Each engagement will have a dice roll with numerical or statistical advantage granted to the player with more dedicated training or higher capability sets. This technique should include actions in spectrum, cyber, and space.

Function #7: Deceive Adversary Audiences. Deception has always been critical to military success. It becomes more important in great power competition and conflict. Deception in previous wargames generally focused on concealing friendly forces but should be expanded to assess more effective means of deception through OIE capability areas. OIE can be employed to delay or degrade the enemy's effective employment of forces and to feint the maneuver of friendly forces. The following technique offers a model to expand deception in wargaming.

Wargaming Technique:

- Step 1. Deception capability. Each player receives three cards to allow the placement of unit tokens on or off the board depending on the desired deception effect.
  - Card 1: Feint forces.
  - Card 2: Overload.
  - Card 3: Conceal.
- Step 2. Deception implementation. Before each turn, each player must roll the dice in front of the white cell/adjudicator, but not in front of the opponent. The dice roll will determine the chance of a successful deception. An intended deception must be rolled prior to each turn that requires the enemy to be deceived (e.g., faking Patton's Army for an assault on Pas-de-Calais would have require a roll on every turn until Germany redeployed forces there and the assault on northern France was conducted). Thus, the larger the deception, the less likely it will be successful. Once the white cell/adjudicator determines a successful roll for deception, the team may place unit tokens for their cards in the following manner:
  - Card 1: Successful feint—use a unit token to show the force that the enemy must address.
  - Card 2: Successful overload—tokens for simulated units (but are not identified as simulated units) will be placed on the board.
  - Card 3: Successful conceal—token(s) removed from the board to deny the enemy's ability to orient his combat power on the opponent.

The techniques listed above are not meant to be a direct representation of executing their applicable OIE functions, but a starting point to consistently integrate OIE into wargames, which serves multiple ends. First, instead of simply "doing cyber" or assuming access to critical logistical nodes for operational sustainment, these techniques introduce a framework through which commanders and staffs apply a deliberate approach to the planning and execution of OIE functions with tangible results in a wargame. Further, when considering how critical wargames are to force design and concept development, we can no longer afford to press the proverbial "I believe button" for OIE capability areas when conducting wargames. Commanders need to know how vulnerable they really are to information and precisely how much power they have to project information. Thus, it is imperative that OIE become a deliberate and focused aspect of all wargames.

Notes

[1] Gen Joseph F. Dunford, Jr., (USMC)Ret, "Department of Defense Press Briefing," (brief, Department of Defense, Arlington, VA: August 2019).

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

[3] Ed McGrady, "Getting the Story Right About Wargaming," *War on the Rocks*, (November 2019), available at https://warontherocks.com.

[4] Peter Perla, *Peter Perla's The Art of Wargaming: A Guide for Professionals and Hobbyists,* (Annapolis, MD: United States Naval Institute, 2011).

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

Fine-tuning the *CPG*

An appeal for amphibious interoperability

by LtCol Brian C. Hawkins, USMC(Ret)

>*LtCol Hawkins is an Allied Maritime Analyst, Marine Forces Europe (MARFOREUR), G-5.*

Released in July 2019, the 38th *Commandant's Planning Guidance* (CPG) outlines a future Marine Corps force that both reiterates and redefines the Service's relationship to the Navy. The bold vision prescribed within the CPG sets a challenging course for the Service and largely succeeds in articulating the challenges the Marine Corps must confront in order to maintain relevance and lethality in competition and conflict with a peer adversary. Despite the eloquence and effectiveness of the CPG's call to action, it misses a noteworthy opportunity by failing to identify and explain how allies and partners fit into our emerging concepts or naval integration efforts.

A Blind Spot in the CPG

Unblinking and unequivocal with regard to force design and concept development, the CPG commendably lays out the benefits and challenges of the proposed future course and answers any lingering questions about "who we are" as a Service. "We" are Fleet Marine Forces supporting the Navy in the "fight to get to the fight" as part of a larger maritime campaign. As a result of this expectation, the Commandant instructs the Corps to devise means for tighter naval integration with our Navy counterparts at every echelon. Additionally, the guidance exhorts the Service to redesign the force in alignment with the challenges outlined in the 2018 *National Defense Strategy*, specifically its focus on a "near peer or peer adversary." In the maritime domain, this explicitly indicates a requirement to contend with the so-called anti-access/area denial (A2/AD) threat possessed by pacing threat forces.

The Marine Corps should build capacity, capability, and interoperability with partners who are there when the fighting starts. *(Photo by 1st Marine Regiment, Swedish Armed Forces.)*

The Marine Corps' primary focus will be toward the Pacific with only modest references to the "other" near peer adversary: Russia. Alongside a newly redesigned force customized for the tasks of competition and conflict with peer-level adversaries, the Marine Corps must develop nascent operational concepts, including expeditionary advanced base operations (EABO) and its parent concept—littoral operations in a contested environment (LOCE). Simultaneously, the Navy is developing its own emerging concepts, including distributed maritime operations and electromagnetic maneuver warfare.

But there is a problem. It is impossible to envision this future conflict with the U.S. Joint Force "going it alone" against China or Russia. A near peer warfight is inherently a combined warfight. A worthy refinement to the sage advice of the CPG would be an invocation to execute design and development efforts *in concert with allies and partners* on the basis of the following five points:

Build effective interoperability. High-end warfighting imagined in future conflict scenarios implies integrated interoperability. Ships, aircraft, landing craft, communications, and command and control (C2) systems from different nations must be able to operate and fight interchangeably.[1] Building and maintaining interoperability to this high standard requires deliberate, multinational planning, which results in alignment of ends, ways, and means across our various partnerships. Some aspects of this integration will be expensive, but less costly than the failure that will necessarily result when allies cannot shoot, move, and communicate together. Other aspects will prove surprisingly affordable and relatively easy to incorporate into existing multinational and bilateral exercises with existing resources.

Develop emerging concepts together. Advanced tactics and processes, such as how to establish an expeditionary advanced base in an A2/AD environment, require discussion, wargaming, experimentation, and significant rehearsal before ever developing the doctrine. The Marine Corps cannot afford the wasted time or energy of building these concepts in "United States-only" seclusion, only to then introduce these concepts to our allies and expect timely implementation several years later. Moreover, the sheer scope and sale of operations as envisioned under distributed maritime operations, in which multiple "fleets" are commanded and coordinated over vast distances, will necessitate leveraging allied and partner capacity during large-scale naval exercises. Opportunities abound to align our emerging concepts with several highly capable partners. Examples include the United Kingdom's Royal Marines' *Littoral Strike* and *Future Commando Force* concepts and the Dutch Marine Corps' *Future Littoral Operating Concept*.

Don't reinvent the wheel. Many U.S. allies and partners currently operate with weapons, vehicles, and equipment that the Marine Corps does not possess but is interested in procuring. One can think of this as "building partner capacity"in reverse. Examples of partner nation capabilities and capacities that exceed those of the United States include long-range precision fires (coastal defense cruise missiles and ballistic missile systems), mine/counter-mine (MCM), riverine and littoral craft, and diverse varieties of maritime connectors. Furthermore, these nations already experiment with these fielded systems in low-signature and degraded communications environments. A bit of humility is in order as the Marine Corps learns from—and aligns its concepts with—allies and partners who are eager to pair with them.

Develop allies as "stand in forces." Another emerging concept the Marine Corps is developing is a concept for stand in forces: requirements, planned activities, and processes for the mix of survivable, risk-worthy, and lethal forces that stand in the enemy's weapon engagement zone once kinetic action begins. While the Marine Corps imagines itself as this force, perhaps a better constituent for this role is the national defense forces of the countries that lay within this vulnerable area. Put simply, our allies and partners *are* the stand in forces. This is particularly true in the European theater: NATO allies and other European partner nations live in the weapon engagement zone and are not moving when fighting begins. Understanding their playbook now—before a crisis—will be just as vital as writing and eventually sharing our own.

Conduct forward-based training. While the Marine Corps typically envisions completion of pre-deployment training in the continental United States as the acme of unit readiness, a strong case can be made that training "in-theater" is preferable and, in some cases, even superior in quality. Limitations on live fire ranges, landing zones, drop zones, and beach landing sites across many foreign littoral training areas tend to be less restrictive than in the continental United States. Additionally, by exercising abroad, U.S. forces gain awareness and experience in future areas of operations alongside prospective partners in near peer conflicts. Furthermore, overseas exercises widen the aperture of total training opportunities and available partner forces. For instance, U.S. naval forces training in conjunction with a riverine craft unit or MCM unit from a small European nation could present valuable long-term benefits; yet this foreign force may find it unreasonable or unaffordable to attend Exercise BOLD ALLIGATOR on the east coast of the United States.

Strategic Reasons for Prioritizing Interoperability

Any serious attempt to build stand in forces should begin with allies and partners, particularly those with high-end amphibious capabilities. The task of the Marine Corps should be to build capacity, capability, and interoperability with partners who are there when the fighting starts. This effort should seek to yield cohesiveness, understanding, and effectiveness across our partnerships. Two side benefits of cross training our allies in our own planned activities, tactics, and processes are fewer requirements for forward deployed Marines and greater distribution of friendly forces across the battlespace at the commencement of any future hostilities.

Additionally, as a practical matter, U.S. naval forces have a tremendous incentive to learn to fight effectively with allies who will fight with us anywhere. While the CPG identifies the challenges in the Pacific as a key focus of effort, we must not neglect the tremendous opportunities offered by Europe. Specifically, no other theater offers highly capable amphibious partners who can and will deploy outside their own theater to fight by our side. Building allied interoperability—from practicing basic skills to developing advanced tactics, techniques, and procedures—renders unqualified benefits for America's warfighting readiness.

Finally, our strategic guidance highlights the need for burden-sharing amongst our allies and partners. A renewed campaign pursuing amphibious interoperability supports the efforts by national leadership to strengthen the team by making all the respective players more capable, effective, and cohesive. In so doing, we reinforce our core strengths by reassuring allies and deterring adversaries. This confounds the adversary strategy which, at the pre-conflict/competition level, is to split America from her allies.

The Way Ahead for Amphibious Interoperability

The Marine Corps, the entire Joint Force, and our allies and partners seem to be in violent agreement that interoperability is an obviously desirable, positive endeavor. What is not as clear is how to attack this objective in a comprehensive, affordable, and persistent way. While procurement of interoperable systems often carries a substantial price tag, training to standards for integrated operations can often be conducted for relatively low cost with high-payoff opportunities for the Service. Two current initiatives aligned to amphibious interoperability efforts merit the Service's attention and prioritization.

Amphibious maritime basing and interoperability (*AMBI*). NATO and other European partners possess significant quality and quantity in their domestic amphibious forces. While U.S. L-Class shipping availability is at a premium, Europe offers approximately twenty-five high-end amphibious ships, many of which could potentially support MV-22 operations. AMBI seeks to "operationalize" interoperability. By building discrete capability roadmaps for a variety of deployment options, AMBI codifies the framework of processes and authorities required for execution by, through, and with our amphibious partners.

Starting with a specific operational endstate (i.e., a specific mix of deployed forces during a specific timeframe), AMBI provides the Service's institutional basis for resourcing and prioritization of interoperability activities by specifying discrete events which must be planned, coordinated, and executed by Marine Corps forces in conjunction with allied or partner nations. Over time, the execution of progressively challenging interoperability events will cross a threshold, demonstrating and validating a desired operational capability. In time, AMBI will allow Marine Corps forces to leverage existing high-end amphibious allies and partners by distributing more Marines across more platforms globally. Ultimately, AMBI offers increased operational flexibility by providing more options to commanders and national decision makers.

The AMBI initiative coincides neatly with the CPG's call for new employment models and a variety of deployment options. Additionally, the timing of AMBI's evolution aligns with Marine Corps force design efforts and development of emerging concepts. Training and integrating with the same partners we will need for any near-peer maritime conflict affords U.S. naval forces with a venue for low-cost support to national and Service strategy and priorities, alignment with geographic combatant commander country objectives, and promotes allied and partner contributions to collective security.

NATO Amphibious Leaders Expeditionary Symposium (NALES). NALES began as a simple "community of interest" for amphibious partners in the European theater but has evolved into a major initiative spearheaded by NATO's Allied Maritime Command. It offers the Alliance the ability to leverage the inherent readiness and flexibility of existing amphibious capacity within NATO. In addition to the robust quantity and quality of amphibious ships across Europe, our allies and partners possess numerous amphibious and naval infantry brigades. Like all amphibious forces, host countries tend to maintain these forces at healthy readiness levels. As a result, several amphibious task groups (ATGs)[2] could be available to NATO for crisis or contingency on fairly short notice.

In the event of a large-scale conflict such as an Article V situation, NATO sees value in leveraging these existing forces. But that many discrete amphibious task forces poses a problem for the receiving fleet or maritime component commander (MCC): NATO does not possess the C2 architecture or doctrinal framework to handle an amphibious task force of this magnitude. In other words, NATO has multiple, multinational ATGs to offer on short notice, but the MCC will not be able to C2 them all independently while running the sea control fight and everything else for which he has responsibility.

NALES provides an intermediate commander amphibious task force/commander landing force headquarters between the MCC and all the subordinate ATGs to handle the amphibious workload on behalf of the MCC. Robust experimentation and rehearsal during existing exercises with existing amphibious forces can and should be conducted at a relatively low cost. Just as AMBI ensures tactical-level interoperability between Marine Corps units and amphibious allies and partners, NALES must be resourced by the Service during every large-scale amphibious exercise in order to rehearse the operational-level maritime C2 envisioned and demanded under our emerging naval concepts.

Conclusion

The CPG is already being lauded for its breathtaking boldness and audacity. It truly is revolutionary and promises to ensure the Marine Corps' relevance and utility to the Nation for years to come. No single document could be expected to address all aspects of future warfighting. It is incumbent upon leaders to identify blind spots and potential opportunities for improvement. To this end, the Service must include allied and partner nation contributions as it matures the future naval force. Minor investments early in resourcing multinational interoperability efforts, as discussed above, will pay dividends over the long run.

A near-peer fight as envisioned by the CPG requires a multinational coalition. The Marine Corps should lead the joint force in preparing for this contingency by bringing allies and partner nations into the discussion. Emerging concept development, learning from allied acquisition and procurement experiences, developing and experimenting with new employment models, and ultimately training to fight via integrated interoperability with our closest and most advanced military partners is simply common sense.

Notes

[1] NATO defines three categories of interoperability. "De-conflicted" interoperability means units can co-exist safely but without interacting. "Compatible" interoperability implies the ability to interact with each other in the same geographic area while pursuing a common goal. The highest level of interoperability, "Integrated," requires interchangeability or the ability to merge seamlessly.

[2] NATO ATGs differ in size and composition. Typically, they will consist of one to two amphibious warfare ships with an embarked marine or naval infantry landing force. While smaller and less capable than a comparable U.S. amphibious force, such as an ARG/MEU, these foreign ATGs are deployed regularly for a range of military missions and maintain inherently high readiness levels relative to their non-amphibious counterparts.

Company Command

What I learned

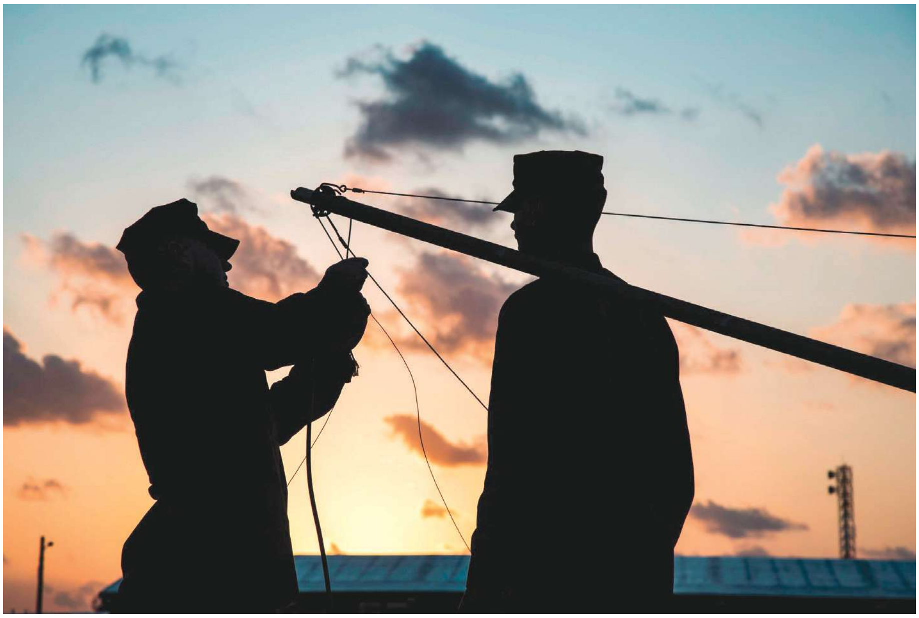
by LtCol Arun Shankar

>*LtCol Shankar is the Assistant Chief of Staff, G-6, 1stMarDiv. He wrote this article when he was the CO, Communications Company, 1stMarDiv. He has also served a combined 28 months in OIF/OEF as a counter-IED Analyst, Assessments Analyst, and Communications Officer, and holds a Ph.D. in Operations Analysis from George Mason University, Fairfax, VA. This summer, LtCol Shankar will assume command of Communications Training Battalion.*

During my six years as a major, I had the great fortune of serving as a communications company commander in two different companies from two different elements of the MAGTF for a total of three years. My experience allowed me to see company command from a field grade perspective and learn from it with a uniquely mature lens. Therefore, I offer three lessons from this experience. First, I suggest that the primary duty of a field grade commander is to affect command culture, not operations. Second, I determine that the field grade rank offers a unique opportunity for the mentorship of both SNCOs and officers, and this opportunity should be deliberate and impactful. Lastly, I share some peculiarities about communications units and how the highly technical missions of these commands present unique challenges.

Culture

Command culture is the enduring spirit within an organization that allows Marines to regularly achieve their operational mission. It is an indirect path to operational success, but it reinforces maneuver warfare and independence at the lowest levels. I have no qualms about the importance of operations and realize that execution within an MOS is a Marine's primary contribution. However, culture outlasts temporary leadership fashions like burdensome micromanagement or the requirement for repetitive feedback cycles. A strong culture sets the tone for hard work and success without the utterance of those words. Most leaders already know this. However, we often struggle with how to create this type of culture. Rookie commanders may think that random, uncorrelated efforts like family socials, field meets, and days off will automatically make Marines happy, therefore resulting in higher mission effectiveness. In my experience, these are recipes for failure because they are focused on short-sighted, immediate results. More seasoned commanders might focus on ruggedizing Marines through tough training that brings them together. This type of change takes longer and requires deliberate planning and assessment that is beyond hopeful experimentation.



Meaningful cohesion is established with the platoon. (Photo by LCpl Christian Ayers.)

Culture is implemented differently in organizations based on how they are composed. Simon Sinek, a well-known optimist, has made a living explaining that the effective messaging of a commander's intent is all that is needed to create a successful organization, and everything else will fall in place. Perhaps this model works well in the profit-oriented business world, but it is only the start of an effective command in the military. The youth of our force, combined with the dangerous nature of our mission, does not yield an environment where boundless creativity and unsupervised action is appropriate. A military command must be structured, disciplined, and resilient. Marines need to be able to do things they do not otherwise want to do, and do those things well. They need to be comfortable being uncomfortable, and they need to be able to lead and manage their subordinates in the same way. Therefore, Marines need to be continually trained and held accountable for their performance in a strict and purposeful manner. To rely solely on the hope that a clear intent will be executed without some level of deliberate management is absolute nonsense.

One of the easiest ways to positively alter culture is to reinforce basic discipline and military traits. Company first sergeants exist primarily for this reason, and that is why they are the commander's primary advisor. Their repeated emphasis on customs, courtesies, uniforms, physical fitness, and overall military standards automatically creates this atmosphere. Consequently, Marines who perform in such an environment naturally develop resilience and problem-solving skills that are necessary in a wartime environment. Furthermore, prescriptive counseling and inspections demonstrate interest in a subordinate's performance and progression. Admittedly, I did not originally believe that an emphasis on garrison standards that are seemingly unrelated to operations would have a positive effect across varied lines of effort. However, after three years of observation, I am convinced there is no other way.

Culture goes hand in hand with morale. But morale is not simply broad happiness. Marines typically are not happy to go on hikes, wake up at 0500, or go to the field when it is raining. In fact, I argue that many tasks in the military fall under this category. Therefore, if these tasks are being executed without artful leadership and teamwork, morale will not be high. I am surprised when Marines tell me that long work days and field operations are surprisingly making them unhappy. That should not be unusual. However, young Marines who do not have leaders who regularly inspect and care about them will sense a void that they cannot always illuminate. This void often manifests itself as a routine morale complaint rather than a desire to be challenged further.

Trust, when defined and implemented properly, positively affects culture. Marines should be trusted to execute tasks by teaching them and then holding them accountable to performance. Trust is often mischaracterized as allowing Marines to operate freely without guidance or supervision. Contrarily, trust allows a Marine to execute a task within finite parameters, followed by verification. As performance improves, the detail and regularity of these inspections can subside. Most Marines are likely to excel when trust is earned rather than given.

A strong command culture does not necessarily correlate with cohesion across the entire unit. Within communication companies, platoon missions are so disparate that true commonalities between them can rarely be identified. A cursory level of competition and excitement can be bred between them, but the meaningful cohesion is established within the platoon, beginning with the platoon commander. A primary role of the company commander is to mentor the platoon commander to develop and maintain this military culture. This deliberate process should be taught to the platoon commander, much like a teacher does for students.

Different elements of the MAGTF have different command cultures. The division is the most unique of them all, as it is primarily focused on rugged training and tough leadership that is common among combat arms MOSs. Additionally, unlike other elements of the MAGTF, every infantry battalion and regiment in the Marine Corps is on a regular deployment rotation. In other words, service in those units will guarantee a deployment, whereas service in other elements of the MAGTF will more likely result in a stateside tour. Furthermore, since SNCOs and officers within the communications fields are encouraged to serve in every element of the MAGTF, the present duty station of such a leader is likely the first time he has served in that element of the MAGTF. Field grade officers have the experience and authority to comprehend this dynamic and address it with new leaders upon arrival. In my experience, this very direct and personalized set of expectations usually put mid-level leaders on the right track immediately. Conversely, the absence of these introductions regularly led to mismatched expectations and suboptimal outcomes.

Mentoring Officers and SNCOs

A field grade commander usually has the privilege of having at least as much time in service as most of his SNCOs and all of his officers. Consequently, he should have the experience and confidence to assuredly mentor SNCOs and officers across the entire command with impact and certainty. Unlike a young, inexperienced captain, a field grade commander should understand the mechanics of platoon management, the dynamics of SNCO-officer relationships, and the art of quality staff work. With this level of cognizance, this commander should be able to anticipate almost all common pitfalls of platoon-level leadership and address them before they occur.

Most of the officers within a command are usually lieutenants who do not have prior military service, so they must be actively mentored. They require immediate and direct mentorship because they are learning both how to be officers as well as how to be Marines. Additionally, they are usually in charge of platoons that cannot be run without adequate leadership and managerial skills. Though SNCOs are often the driver behind this effort, lieutenants are formally in charge. Therefore, they need to be held accountable to enforce the commander's intent and deliver results. This mentorship is often effectively delegated to captains who are exceptional at teaching lieutenants the mechanics of leadership and management. However, broader institutional thoughts and lessons learned should be regularly shared by the field grade commander. In my experience, a field grade commander's greatest responsibility is the mentorship and evaluation of his lieutenants.

Within the communications MOS, it is also common to have warrant officers within the unit. Unlike lieutenants, these officers are very experienced and usually have technical expertise that far surpasses anyone else. However, uniquely within a company structure, these warrant officers also often have limited experience as officers. They may struggle with understanding the difference between a SNCO and an officer, tackling platoon-level tasks as they arise rather than planning, and anticipating larger initiatives that support a wider intent. They are also usually unfamiliar with the unwritten rules of staff work and the most efficient ways to derive decisions from a commander. The field grade commander is the uniquely qualified person in the command to foster this mentorship and coach these officers into future roles as advisors and planners for major subordinate command- and MEF-level staffs.

> ***Most leaders would argue that field grade officers do not play a role in SNCO mentorship, but after three years of company command, I wholeheartedly disagree with this premise.***

Most leaders would argue that field grade officers do not play a role in SNCO mentorship, but after three years of company command, I wholeheartedly disagree with this premise. In fact, I now argue that it is one of the most essential roles of a field grade officer. A unit cannot operate with substandard SNCOs, so this absolutely critical single point of failure deserves the daily attention of the seasoned commander. Senior master sergeants/first sergeants and master gunnery sergeants/sergeants major certainly play a role in this mentorship formula, but the direction and priority of this leadership is the responsibility of the field grade commander.

Peculiarities of the Communications MOS

The communications MOS is one of the most unique ground combat support MOSs in the Marine Corps. The highly technical aspects of the MOS make it nearly impossible for SNCOs who exit the MOS to return with meaningful proficiency without significant initiatives in self-study. This often leads to a lack of confidence, which can then trickle into an inability to manage and lead subordinates. For most SNCOs, it is not natural or practical to ask their Marines to teach them how to employ new equipment, so choices are limited on how to mitigate this challenge. Most bases provide refresher training courses that can reintroduce the SNCOs to the equipment, but the most effective way to regain proficiency is by going to the field on a regular basis. Field exercises generally require the setup and teardown of tactical networks, so they are the premier opportunity for growth in MOS proficiency.

Unrestricted officers are also challenged within the MOS. Unlike many other MOSs, communications officers are not taught and not expected to emulate the MOS skills that their Marines possess. The amount of time it takes to develop those skills across every communications MOS is inordinate and impractical. A platoon commander likely has a strong understanding of how to plan a network and the critical challenges among equipment and personnel, but he probably cannot program a switch, router, or server to function on that network. This supervisory shortfall is amplified when the SNCOs also lack an understanding of the employment of the equipment.

Moreover, like any technical MOS, the culture of the Marines within the ranks is unique. Marines within the communications MOS are extremely intelligent, willing to challenge ideas, and generally find pleasure in operating their equipment in a field environment. The constant training required to remain proficient often prevents these Marines from honing their warfighting skills to the same level. In this setting, unless the commander prioritizes the "whole Marine concept," these skills can atrophy and thereby negatively alter the culture of the unit.

Conclusion

As I write this, I conclude my time at Communications Company, 1st MarDiv, arguably the finest communications outfit presently in the Marine Corps. This unit of almost 300 Marines has not had a DUI in nearly 700 days, has not woken up their CO for a Commander's Significant Notification Event in the last 6 months, and recently received the LtCol Shea Memorial Unit Award from HQMC C4: the award presented to the unit that made the greatest contribution to the communications community in the last year.

Operationally, the company has never been better. Our Marines recently deployed the first ever wireless, garrison NIPR network to a combat operations center in the field. They also innovated technologies to significantly decrease the electromagnetic footprint in the field without diminishing essential communications services. Moreover, our company is the unit of choice for the field testing of experimental capabilities, and our NCOs are constantly innovating new ways to improve tactical communications.

With all due respect to my outstanding young Marines, these accomplishments did not happen by accident. Perhaps we were staffed with exceptional leaders or unusually reliable equipment, or we just had a very good crop of young Marines. But what is more likely is that our leaders adopted a culture solely focused on hard work and mission accomplishment, and that emphasis trickled down to our Marines. They then took intent and executed it brilliantly. I am so proud of them, and so proud to have been on their team.

I will miss my Marines as well as Communications Company. Command truly is the greatest privilege an officer can ever have.

Preserving the Force Through Leadership

Know your Marines and look out for their welfare

by Col Michael Styskal & Dr. Marta Garrett

>Col Styskal was the CO, 3d Marine Regiment, Kaneohe Bay, HI, when this article was written.

>>Dr. Garrett was the Embedded Preventive Behavioral Health Capability (EPBHC) Prevention Specialist when this article was written.

The Marine Corps is known for its ability to win in combat: *any mission, anytime, anywhere*. More than any weapon they might carry, the Marines themselves have always been the critical guarantors of this success. Marines are what makes the Marines Corps unique. The Marine Corps' practice of making Marines involves a complex and dynamic values-based transformation that is essential to the institutional *esprit de corps*. This transformation begins when Marines step onto the yellow footprints or raise their right hand to swear their oath, and continues every day they wear the uniform. Preserving this force of ever-ready and always-capable Marines requires constant leadership effort. Increasingly, Marine leaders face new and complex challenges in looking out for the welfare of their Marines in garrison, much less on the battlefield. Human factors such as pre-service experiences and current stressors can break down the resiliency of even the strongest Marines, making them less effective and less ready. Thus, it is incumbent on all levels of leadership within the Marine Corps to embrace the leadership principles which enhance force preservation to build and maintain a more ready and lethal force. This article describes both the evolution of the force preservation process at the unit level as well as leadership best practices to help ensure proactive command support for all Marines.

Preserving the Force Through Leadership

Where the primary objective of Marine Corps leadership is to accomplish the mission, the secondary objective is the welfare of the Marines being led.[1]

The Marine Corps' culture and philosophy views every Marine as a leader. In becoming a Marine, each leader is indoctrinated with the core values of the institution including the eleven Marine Corps' Leadership Principles and the fourteen Leadership Traits (see Figure 1). These values serve as a guide for all aspects of leaders' behavior within the Corps, making it is essential to understand the need to preserve the force as a form of Marine leadership. Preserving the force is clearly spelled out in the Leadership Principle: *Know your Marines and look out for their welfare*. As Gen John A. Lejeune stated, "leading Marines involves connecting with them and working to understand what motivates and drives them."[2] The Marine Corps describes this as engaged

11 Leadership Principles	14 Leadership Traits
Know yourself and seek self-improvement.	Justice
Be technically and tactically proficient.	Judgment
Know your Marines and look out for their welfare.	Dependability
Develop a sense of responsibility among your subordinates.	Initiative
Keep your Marines informed.	Decisiveness
Set the example.	Tact
Make sound and timely decisions.	Integrity
Seek responsibility and take responsibility for your actions.	Endurance
Ensure assigned tasks are understood, supervised, and accomplished.	Bearing
Train your Marines as a team. Employ your command in accordance with its capabilities.	Unselfishness
	Courage
	Knowledge
	Loyalty
	Enthusiasm

Figure 1. Marine Corps Leadership Principles and Traits.

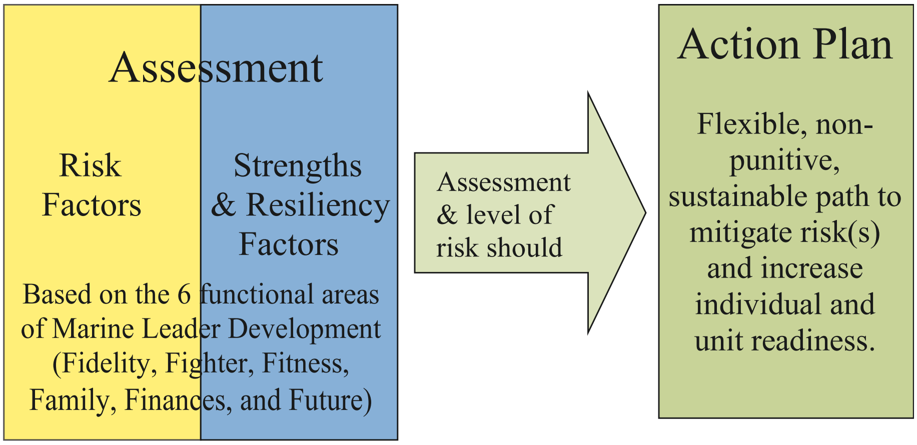
leadership or values-based leadership which is essentially the practice of mentoring and taking care of the individuals within one's charge, looking out for their welfare, and inculcating them to the organizational culture and values.

Force preservation is essentially a verb describing these actions taken by effective Marine leaders at all levels to ensure that the welfare of Marines is looked after and that they are always ready and able to assume the responsibilities given to them. The formalized side of preserving the force, or the *Force Preservation Council* (FPC), has been around for over a decade, and the Marine Corps order mandates a monthly review to assess potential risks and mitigate these risks through appropriate leader action.[3] This force preservation review process was designed to help commanders address critical individual and unit risk factors that could possibly interfere with readiness. Because Marine commanders are not typically subject matter experts in behavioral health, the FPC guidance and structure encourages input from small unit leadership, medical and behavioral health providers, and readiness enablers to support commanders in making informed decisions about how to best assist Marines and buy down risk to the force and mission. Functionally, the standardization of the FPC process attempted to operationalize the decades-old values-based leadership of Marines taking care of Marines by ensuring monitoring and accountability in today's busy and complex command environment.

Assessing Risk and Resiliency

Fundamentally, the force preservation process aims to assess and mitigate potential risk factors to enable commanders to make necessary decisions about deployability, safety, and personal development. While leaders at all levels are involved in this assessment and mitigation process, only the commander owns the mission and thus is essential for the commander to fully understand all potential risks within the command. To be effective, the risk assessment process must consider the individual Marine's strengths and resiliency, in other words, the Marine's ability to bounce back in adversity (see Figure 2). The eleven Marine Corps Leadership Principles and the fourteen Marine Corps Leadership Traits offer direction to help leaders fully assess Marines' strengths and resiliency or ability to persevere. Without this added strength-based perspective, any risk assessment would be incomplete and only provide the commander with the glass-half-empty view, which may not be sufficient to guide the commander's required decisions.

Unfortunately, this assessment process is not as simple as this description alludes. Successful force preservation requires a multidimensional risk mitigation approach to not only assess individual factors of Marines but also to maintain situational awareness of unit and environmental factors that have the potential to influence the risk mitigation process.


Assessment

Risk Factors

Strengths & Resiliency Factors

Based on the 6 functional areas of Marine Leader Development (Fidelity, Fighter, Fitness, Family, Finances, and Future)

Assessment & level of risk should

Action Plan

Flexible, non-punitive, sustainable path to mitigate risk(s) and increase individual and unit readiness.

Figure 2. Framework for decisions about force preservation.

Assessing the Marine. In this context of preserving the force, the goal of leadership within the Marine Corps could be described as transforming and developing Marines to prepare them to win in combat. While this end state does not change, the path to achieve it must recognize the need to adjust fire from time to time. Senior leaders are likely to attempt to engage and assess their Marines from a *legacy* perspective—relying on traditional expectations and interaction styles that were commonplace as they entered the Marine Corps. But the Marine Corps is an exceptionally young force that turns over very quickly. Today's cadre of young Marines is qualitatively different from any previous cohort of Marines. While they may share many characteristics with the generations of Marines who served before them, they are also very different. Today's Marines are digital natives raised with very different developmental experiences and expectations. They view themselves and their service differently and they interact with each other and the world around them differently than previous generations of Marines. Acknowledging these differences can require a fundamental shift in leadership perspective to better understand differences in motivation, communication styles, and interpersonal skills of today's young Marines. The leadership challenge is to retain a positive focus because difference does not equate to weaker or less desirable. This speaks to the leadership principle of *knowing oneself.* It may be easier to focus on a potential weakness rather than working to understand how something (like being a digital native) can bring strength to the team.

Assessing the unit. Comprehensive force preservation assessment must also consider the unit. Each unit within the Marine Corps has specific characteristics that have the potential to impact risk and resiliency and create challenges for force preservation decisions. Commanders must be well-informed and open to exploring how individual unit characteristics and demographics can impact force preservation issues. For example, a "young" infantry unit may have many more first-term, single Marines (perhaps as many as 40-50 percent of the total unit may be under legal drinking age). Without an understanding of the pre-Service stressors young Marines bring into the unit (e.g., adverse childhood experiences or ACEs), command leadership is at a distinct disadvantage in trying to fully assess risk factors. Additionally, this young group often faces financial hardships, has not fully internalized Marine Corps' institutional values, and may struggle with a host of adjustment issues such as homesickness, regret at joining the Marine Corps, or struggling to carve out a sense of independence from extended family. Marines who come from dysfunctional families are particularly at-risk in this phase of adjusting to the Marine Corps and living up to Marine Corps values. While some may see the Marine Corps as their best opportunity to escape issues they faced in childhood, others may lack social skills and knowledge about how to make needed adjustments to be successful during this transitional period. This young group of Marines is also more susceptible to developmentally typical at-risk behaviors such as substance misuse, intimate partner abuse, and poor decision making. When Marines in their first enlistment hit a bump-in-the-road, they are often more likely to want to bail from the Marine Corps rather push through the hardship and complete their enlistment contract. In these situations, behaviors of individual Marines can quickly interfere with unit moral and cohesion as they focus on getting out of the Marine Corps vice internalizing the Marine Corps values. This creates a unique leadership demand raising the question: *when does taking care of your Marines and looking out for their welfare become secondary to the unit?* (Which speaks to the leadership tenet of training your Marines as a team.)

Alternatively, a headquarters unit or aviation unit might be staffed with more senior leaders, more educated Marines, and may include more married Marines and families with children. This older group of Marines is more likely to have adjusted or rebounded from potential pre-Service stressors and has typically embraced the Marine Corps' values at least to the extent that the institution is providing for their financial needs. However, these Marines may also feel they have more to lose. Rank and experience also increase the expectation level, and these Marines may be experiencing a stronger fear of failure—creating higher levels of anxiety and stress. Additionally, experience in the Marine Corps also brings about knowledge of processes in the Marine Corps, meaning these Marines may still be engaging in at-risk behaviors, but they are likely to be better at hiding maladaptive behaviors. Thus, when a more senior or more educated Marine faces challenges, these issues are more likely to be protracted or complex to mitigate. When the command team engages leaders at all levels and all Marines are assessed routinely—regardless of rank or position—this opens the potential to catch risk left of bang or before an incident blows up beyond repair.

Finally, the unit's training exercise employment plan (TEEP) may also provide essential cues for understanding work-related stressors and how these stressors could potentially impact force preservations or readiness. Often unit leadership can be slow to detect everyday work stress caused by a busy TEEP or hectic work environment because leaders are often isolated from some of these experiences. However, nearly three quarters of military families feel the current operational tempo exerts an uncomfortable level of stress, enforcing the idea that military life in general is stressful.[4] Inspections, frequent duty, long work hours, poor or changing junior leadership, and gaps in filling key billets can add work stress at levels that commanders may not see without specifically looking for key indicators. Deployments or field exercises typically create anxiety for Marines who have never experienced these events but can also increase stress for even the most seasoned Marines. To help mitigate these TEEP-related issues, engaged leaders must realistically anticipate the needs of their unit for down time and *set the example* with an informed leave/liberty policy that allows Marines down time as they transition in and out of the unit.

Assessing the environment. As described, force preservation decisions are complex. In addition to assessing the individual Marine and the unit, engaged leaders must also gain situational awareness of other environmental factors even if these factors are outside the scope of the individual leader or even the Marine Corps. For example, the location of a unit can provide hints to potential after-hours and liberty risks for Marines. Commanders outside of the United States have more ability to restrict liberty if needed or to create liberty policies designed to reduce risk. Commands near locations known for partying or illicit activities may face unique challenges in addressing these risky attractions. It is critical that each commander know potential risk factors that lie outside the gate: *What is the drug of choice in this community? How might this impact Marines? Who in this command is potentially at risk?* Armed with this type of knowledge, commanders can tailor liberty and safety briefs to address specific risk factors in the same manner one might address local intelligence risks.

The 6-Fs as They Relate to Preserving the Force

Over the last decade, force preservation has evolved with little additional guidance from HQMC. Commanders have learned by trial and error what has been helpful to them to buy down risk through mitigation. A recent trend in the force preservation process has been to incorporate the six functional areas (The 6Fs) of the Marine leader development literature (fidelity, fighter, fitness, family, finances, and future) to ensure assessments are comprehensive and better inform the mitigation process. To support commanders in considering force preservation as it relates to each of the 6-Fs, the following examples of risk factors, related strengths, and leadership characteristics are provided.

While these descriptions are not all inclusive, they are offered as a guide to understanding how a comprehensive risk and strength assessment might look along the 6Fs. The importance of the 6Fs in force preservation is to ensure a thorough and broad assessment using a *strengths-based approach* that covers

6-Fs	Brief description	Examples of risk factors	Examples of strengths and resiliency factors associated with Leadership Principles or Leadership Traits
Fidelity	Core values, expectation of ethical conduct.	Legal, disciplinary, and guidance issues.	Taking responsibility for ones actions. Bearing. Integrity.
Fighter	Skill-sets and knowledge that makes Marines into warriors.	Performance or communication difficulties; challenges in meeting required training standards.	Being team-oriented, open to feedback. Tact. Being technically and tactically proficient. Knowledge.
Fitness	Four chords of total fitness; and adaptability to transitions.	Issues with appearance standards, emotional control, health concerns, addictive, or self-isolating behaviors.	Enthusiasm. Endurance. Initiative. Set the example. Employ command in accordance with its capabilities.
Family	Family of origin and current relational issues (spouse, partner, children, friends).	Pre-service experiences; recent change in relationship status; cross-cultural relationships, etc.	Loyalty. Dependability. Unselfishness. Setting the example. Developing a sense of responsibility.
Finances	Personal financial responsibility.	Financial challenges, poor credit, excessive spending or bills.	Judgment. Taking responsibility for ones actions.
Future	Setting and accomplishing goals.	Lack of goals or unrealistic goal setting; inability to move towards goal accomplishment.	Decisiveness. Judgment. Initiative. Knowing yourself and seeking improvement. Making sound and timely decisions.

Figure 3. The 6-Fs of leadership development, risk assessment, and strengths.

all major components that could create potential risk. In-depth knowledge of one's Marines allows for a more realistic understanding of how much hardship or difficulty each Marine may be capable of tolerating without bringing additional risk to mission or self. Thus, when commanders consider not only risks but strengths, leaders are able to create a mitigation plan that is more realistic and achievable and can *employ the command in accordance with its capabilities*. This assists the commander in buying down overall risk to force or mission.

Creating a Leadership-based Action Plan

A leadership-based action plan can be considered like an operational risk management worksheet. Once the force preservation assessment has been completed, the way ahead is established through an action or mitigation plan which is used to implement controls and serve as a roadmap to assist leadership in taking care of their Marines. Understanding where Marines strengths and needs are in the context of the Leadership Principles and Leadership Traits can also provide guidance to support effective action plans.

Beyond assigning each individual with an overall risk rating (low/green, elevated/yellow, medium/orange, or high/red; [see Figure 4]), leaders should also consider if the risk is consistent, trending toward improvement, or worsening since the last assessment. This is helpful to leaders who may have large groups of Marines to assess and may also assists leaders who need to step into this process mid-stream. As described, the force preservation action plan should also consider the overall assessment of the Marine, the unit, and the environment. Again, an accurate overall risk assessment allows the leader to *employ*

LOW	ELEVATED	MEDIUM	HIGH
• Encourage positive personal and professional growth and maintenance of strengths and resiliency.	• Connect with and engage regularly. • Mentor and monitor risk level to keep situation from worsening. • Support needs.	• Refer to resources and services as needed. • Monitor progress frequently. • Re-evaluate risk often and adjust plan as needed.	• Refer for professional assistance (medical and behavioral health). • Monitor closely. • Support reintegration or separation as required.

Figure 4. The focus of the force preservation action plan.

the command in accordance with its capabilities. Because force preservation is a non-punitive process, any documentation of this assessment and plan of action serves only to inform the commander and track what has already been done and what actions will be taken in the future.

Marines in the green zone are considered *ready* or *good to go*; while it may be easy to overlook green-zone action plans because they are not essential to safety or risk mitigation in the moment, green zone plans are essential to overall force preservation and maintaining the strength of the force. Action plans in the green zone are essential to help grow and develop talent of the best and brightest Marines to ensure they are encouraged to be successful in the Corps and remain in the Marine Corps. Green zone leadership action plans may support team building, mentoring, or measures the Marine can engage in, such as additional training, education, or other professional and personal development opportunities.

It is arguable that most Marines live in the yellow zone because of the high operational tempo and the unique demands of Marine Corps life. Leadership action plans in the yellow zone are likely to require additional command leadership involvement or monitoring beyond what is provided to Marines in the green zone to ensure the situation continues to trend toward improvement. Like the example of the operational risk management worksheet, yellow zone activities may include implementing controls that are internal to the command such as safety briefs and performance counseling. Like green zone action plans, it may be easy to overlook the importance of yellow zone action plans because they are commonplace. However, yellow zone action plans are critical to ensuring the Marine gets the help needed to keep the situation from worsening and to mitigate any on-going risk while it is easiest to control—while it is still left of bang.

Leadership action plans for Marines in the orange or red zones will likely need referral to sources of assistance outside the command including professional behavioral health or medical help. While leadership may have less input into helping Marines in the orange or red zones because of the greater need for outside professional help, leadership during these transitional zones is still essential. Marines must be encouraged to get the help they need in an environment that encourages help-seeking, and Marines must be supported as they transition back to full duty (yellow or green zones) or potentially transition out of the Service (if they are not able to return to full duty after assistance and care). Regardless of the zone of the action plan, all action plans should focus on skill building and support with the goal of catching Marines early, intervening, and monitoring.

Best Practices for Preserving the Force

As described, there are significant unit factors that have the potential to negatively impact readiness and the force preservation process. However, there are also many positive characteristics across units that have the potential to mitigate and reduce potential risks. The following list offers broad lessons learned about unit practices that can intentionally or unintentionally impact force preservation and readiness. To mitigate readiness risks, the following unit and general force preservation recommendations should be considered:

- Use the command climate surveys to inform force preservation. Any Marine, despite age, intelligence, background, or training, is susceptible to at-risk behaviors during times of transition as well as times of extreme or prolonged stress. Unfortunately, transitions and stress are common within Marine Corps' life. The command culture can provide key information to assist a commander in assessing risk especially during times of command transition.
- Re-evaluate and update unit check-in and check-out processes. Simplify these tasks whenever possible and ensure the required stops are adding value and helping to identify potential risk factors. Even positive transitions can be stressful for Marines. Emphasize the potential sources of help and assistance during these transitional times when risk is increased. Use the mentor program or the chain of command to ensure transitioning Marines have a workable and realistic written plan to address anticipated needs during their transition(s).
- Regularly update and utilize unit personal readiness checklists to ensure all Marines have a plan in place for military life-cycle transitions and unexpected crises (e.g., family care plan, point of contact for medical emergencies, etc.). Having this document in place *before* an urgent situation occurs

Transitions and stress are common in the life of a Marine. **(Photo by Cpl Bernadette Plouffe.)**

not only helps to minimize potential crises but also helps to keep a dialogue going about help-seeking and resources available to all Marines.

- Increase visibility of and support for the unit's sponsorship program. Engage all levels of leadership to ensure sponsorship goals are known, discussed, and met. Sponsorship takes extra effort and time outside of regular duty responsibilities so leaders should reward sponsors who take this task seriously. Set the expectation that small unit leaders should follow and report on the adjustment progress of all new joins at the 30-, 60-, and 90-day marks to ensure a poor adjustment process is corrected as quickly as possible.
- Ensure that local resource information is provided and posted around the unit. Marines may have heard of differing services in boot camp, at the schoolhouse, or at a previous duty location, but may not think to look for these same resources in a new location. Include internal sources of help, such as the Chaplain and the military family life counselor, in all safety briefs, formations, and other unit gatherings to send the message that it is okay to seek help.
- Encourage opportunities to increase resilience without fear of punishment or failure. Resiliency builds more resiliency. Use a step-by-step skill-building and team training model to prepare Marines for upcoming challenges such as deployments or inspections. Ensure Marines are offered the opportunity to express concerns in a team environment that is supportive and encouraging. When Marines are provided positive reinforcement before, during, and after a potential challenge, they are more likely to feel they can take on more the next time. Encourage team building activities and competitions within the larger unit to bond small units and bring outsiders into the fold. Engage Marines in community service not only to help distract them from their own concerns but to help them build useful life skills and provide them with perspective about the resources and strengths they already possess.[5]
- Engage small unit leadership in the force preservation process. Educate leaders at all levels on force preservation processes and expectations. Junior leaders, while they are most likely to know the individual Marine, have not likely had formal training on what is expected of them in the force preservation process (e.g., higher levels of privacy required). Ensure that leaders at all levels understand that the purpose of force preservation is not punitive or evaluative but preventative.
- Maintain a force preservation assessment process that is strengths-based, descriptive, and factually oriented. Risk assessment should not include thoughts, feelings, or judgments; assessments should be on-going, dynamic, and updated as more facts and information are gained. All Marines, regardless of rank or position, should be assessed for risk and strengths because all Marines should be known by their leaders. Resiliency is seen as a positive factor, but the absence of resiliency is easily viewed as a weakness rather than a skill needing to be further developed.
- Finally, consider renaming the force preservation process to emphasize leadership roles and expectations and minimize potential negative connotation. Force preservation must be a leadership-based action or verb—not a noun. If force preservation is seen only as the Force Preservation Council, it brings stigma when Marines are placed "on" the FPC.

Summary

Preserving the force or taking care of Marines is a core Marine Corps leadership function. The force preservation process, regardless of the name, is about looking out for Marines' welfare. It is about leadership. Addressing potential risk factors as early as possible helps to build and maintain a stronger, more ready, and more lethal force. Leadership at all levels—and commanders specifically—must be intimately involved in this assessment process as it helps commanders to buy-down risk. Risk mitigation is not 100 percent fool proof and it should never be expected to catch every at-risk Marine left of bang. Knowing and taking care of one's Marines must be re-emphasized in every level of leadership instruction and formal education program to ensure all levels of leadership develop the necessary skills to accomplish this critical mission. Commanders must step up and help shape the future of the force preservation process through informed leadership and experience. Preserving the force is about leadership not technology. Developing a Corps-wide database tool to track Marine's issues will not make leaders any more effective at assessing or helping their Marines—knowing your Marines will. Complicating the force preservation process with additional digital data keeping responsibilities will likely only frustrate leaders with more tasks and take critical time away from their ability to get to know and lead their Marines. Only emphasizing the Force Preservation Council will bring more stigma and discourage more Marines from seeking help when they most need it. What is required is a re-dedication to the values-based leadership model that is deeply engrained in the culture of the Marine Corps: *know your Marines and look out for their welfare*.

Notes

[1] C.J., Phillips, C.A. LeardMann, K.J. Vyas, N.F. Crum-Cianflone, and M.R. White, "Risk Factors Associated with Suicide Completions Among U.S. Enlisted Marines," *American Journal of Epidemiology,* (Oxford, UK: Oxford University Press, 2017).

[2] Maj Ralph Bates, Jr., "Leadership, John Lejeune style," *Marine Corps Gazette,* (Quantico, VA: November 2014).

[3] Headquarters Marine Corps, *MCO 1500.60, Unit Force Preservation Council,* (Washington, DC: 2006).

[4] Sarah Meadow, Terri Tanielian, Benjamin Karney, *The Deployment Life Study,* (San Monica, CA: Rand Corporation, 2016).

[5] E.H. Erwin, "Community Service and the Marine Corps: Making Better Marines By Building Stronger Communities," *Leatherneck,* (Quantico, VA: December 2013).

Adaptive Thinking

Training for dynamic environments

by Capt Jason Topshe

>*Capt Topshe is an Infantry Officer in the Marine Corps Reserve currently assigned to the Talent Management Oversight Directorate, HQMC.*

"Brilliance in the Basics"[1] is a near universal tenet of combat training throughout the Marine Corps. Mastery of basic skills provides a foundation from which one can learn more difficult ones; more importantly, it allows us to devote our energy to critical thinking in more complex situations when we do not have time to worry about the basics. It allows us to achieve one of the most important tactical concepts discussed in *MCDP 1-3: Tactics*: adapting. This article discusses the complementary relationship of adaptive thinking and brilliance in the basics, as well as ways to create training that prepares Marines to operate in dynamic environments.

Mastering the Basics

As Marines, we seek to master basic skills until they become intuitive and can be automatically performed in any environment. In individual combat-related skills, a key element of this lies in training our senses, most importantly a so-called sixth sense: proprioception. Proprioception, sometimes referred to as the kinesthetic sense, is "the unconscious perception of movement and spatial orientation arising from stimuli within the body itself."[2] It is also defined as "the internal sense of the relative position of the body's musculoskeletal units with each other and the effort needed to move them."[3] Proprioception is involved in all aspects of daily life, from driving a car (how hard to press the gas pedal or the brake, how much to turn the steering wheel), to riding a bike, and even to walking. It allows us to learn new skills and master old ones. Training our proprioception in tactical drills is a key building block to becoming brilliant in the basics of our job as Marines. Along with job-specific knowledge, brilliance in the basics comes in a large part from the mastery of common proprioceptive tasks for a particular job, whether it is firing a rifle, flying an airplane, or driving a HMMWV.

As we gain proficiency in basic tasks, they become more automatic, requiring less mental energy to execute successfully. Think of someone's first time driving a car in traffic. He is probably a little nervous and has to expend a good amount of mental energy thinking about when to speed up, when to slow down, and when to change lanes. After years of driving, however, these tasks become relatively effortless and automatic, allowing the driver to think about his day at work or listen to music. The same applies to military-specific proprioceptive training such as magazine reloads, buddy rushing, or setting up a mortar system. However, not all skills can be truly mastered to the degree that our intuitive judgments will be correct all of the time. By becoming as proficient as possible at the basic things that we *can* master, we will save more time and energy for the complex things that we *cannot* master.

Psychologist Daniel Kahneman identifies two basic conditions required for mastering a skill: an environment that is sufficiently regular to be predictable and an opportunity to learn these regularities through prolonged practice.[4] When it comes to mastering skills for Marines, the problem with these conditions is that the environments Marines operate in are often unpredictable and irregular. There are no rules and regularities that both sides follow as there are in other domains like chess

We gain proficiency by repeated training and emphasizing the basics. *(Photo by LCpl Andrew Bray.)*

or sports. There are, however, many basic skills that are similar regardless of the environment, and Marines can and do master these through prolonged practice. These include basic individual skills like handling a weapon, engaging a target, or calling a fire mission. The real challenge then, once these basic skills are mastered, becomes executing them in increasingly complex and uncertain environments. In the same way a professional wide receiver needs to learn how to run and catch a ball before learning how to run routes against defenders, the basics are stepping stones in learning how to execute in the real world. Designing training that bridges the gap from executing the basics in a predictable environment to executing them in a complex operational environment is a key task of unit leaders.

Bridging From the Basics to Real Life

As a young golfer, Tiger Woods' father, Earl Woods, trained him how to stay focused on the task at hand by dropping his golf bag or jingling coins in the middle of his backswing.[5] He knew that in real competition there would be distractions, frustration, and imperfections. Training with distractions helped hone Tiger's mental strength, and the same types of methods can be used to train Marines.

Immediate action drills can be practiced at home, behind the barracks, or on the range, but it will never be quite the same in these environments as in real life. In real life, the situation will never be as sanitized as it is in training. Every real-life situation will include distractions and elements of friction. Fighting through these requires mental focus. Once Marines become proficient in basic tasks, training should incorporate constantly varied distractions and friction. There are a few simple ways to add complexity to basic tasks to enhance our ability to employ them while working in stressful and distracting situations:

Eliminate a key sense from an activity (e.g., practice weapons handling blindfolded with an unloaded weapon or practice hand and arm signals in silence to train non-verbal communication). Eliminating one sense will improve proprioception and with practice will make these activities feel natural.

Repetition. Devote an hour or so every day to mastering an essential part of your job. This could be transitioning from rifle to pistol, memorizing report formats, or writing orders. Consistent practice builds good habits and trains skills to true mastery.

Varied targets on the range. Not all enemies will look the same, nor should all of your targets. Different colors, shapes, and numbers drawn on targets are sufficient to incorporate shoot/no shoot scenarios, enemies with different weapons, and civilian considerations. A range where yellow targets are enemies with small arms, red targets are enemy machine guns, and green targets are civilians is much more realistic than "shoot everything that pops up."

> ***A range where yellow targets are enemies with small arms, red targets are enemy machine guns, and green targets are civilians is much more realistic than "shoot everything that pops up."***

Practice in different environments and under different levels of stress. Train at different times of day in every kind of environment you can find. Participate in a tactical decision game after running 800 meters, while surrounded by loud noises, and while somebody else is talking to you. Once skills are trained to a significant level of competence in one environment, add complexity and outside factors that force Marines to adapt what they know to the new situation.

Becoming an Adaptive Thinker

In addition to training under constantly varied and difficult conditions, it is also important to think critically and reflect on every training situation to learn and apply lessons for next time. A "hotwash" or after-action review is an essential part of the learning process and not just a box to check. The hotwash needs to be a candid discussion among everyone who participated as to what went right, what went wrong, and how it can be improved for next time.

MCDP 1-3 lists two basic ways to adapt: *anticipation* and *improvisation.*[6] Anticipation can occur when "we have enough situational awareness to understand a situation in advance and take preparatory action."[7] Improvisation occurs when "we have to adapt to the situation on the spur of the moment without time for preparation."[8] Both can be trained through a practice of "action learning" advocated by Dr. Christopher Paparone in an article entitled "Two Faces of Critical Thinking for the Reflective Military Practitioner."[9] Dr. Paparone discusses the differences between two paradigms, the logico-scientific objective (e.g., doctrine, tactics techniques, and procedures [TTP] SOPs) and the interpretivist subjective (dealing with complex, ambiguous situations),[10] and how they relate to "indeterminate zones of practice."[11] Indeterminate zones of practice are the complex, uncertain situations that do not have a clear answer. Few situations in real life can be solved by relying solely on logico-scientific knowledge or solely interpretivist knowledge. Adhering strictly to doctrine or doing it "by the book" rarely works in a complex, ambiguous environment. But we also cannot rely on intuition alone in a complex environment without having some understanding of the underlying doctrine, TTP, commander's intent, and the overall mission. We must be able to work between these two poles in the indeterminate zones of practice, applying knowledge and lessons learned when they work, then adapting as the situation requires. The late Massachusetts Institute of Technology professor Donald Schön offers an analogy on two very different types of professional practice:

We have to train in conditions of uncertainty and stress. ***(Photo by LCpl Andrew Bray.)***

> In the varied topography of professional practice, there is a high, hard ground where practitioners can make use of research-based theory and technique, and there is a swampy lowland where situations are confusing 'messes' incapable of technical solution.[12]

The "swampy lowland" is where Marines will typically have to work; thus, it is where Marines should train so that they become used to dealing with uncertainty. Mastering the basics provides the foundation for dealing with uncertainty, but eventually, we will have to come up with a solution that was not in the training manual. That does not mean that doctrine is useless. We must first know the rules in order to be able to bend and, if necessary, break the rules. We adapt by bending and breaking the knowledge, assumptions, biases, and doctrine we already have. We win by doing this faster than the enemy.

Conclusion

So how do we apply this knowledge to become successful leaders?

Master the basics first. Train in as many of these as possible, until they become almost automatic.

Train under conditions of increasing uncertainty and stress. Get out of your comfort zone. Train in the gray area, the indeterminate zones of practice. Accept that there is often no doctrinal or straightforward answer to complex problems. Every real-life situation will involve unpredictable events and a unique solution. Use what you and your Marines already know, and think critically about what you *don't know* to figure it out. Afterward, reflect and learn lessons for next time.

Accept feedback. Accept it, but do not just nod your head then shrug it off. Think critically about it, and if it makes sense, apply it.

Connect the dots. Everybody will bring unique abilities to the table, and everybody will have strengths and weaknesses. Leverage the abilities of subordinates as well as your own to find a realistic way to accomplish the mission.

Look at the situation from the perspective of an outside observer. To paraphrase an analogy from author Nassim Taleb, imagine a group of tourists looking at a cage of monkeys playing at the zoo and laughing at how silly our ancient ancestors are. Surely, thousands of years from now, some future human will be looking back at *us* and laughing at how stupid *we* are.[13] This second-order thinking is key to helping us make better decisions as well as understanding ourselves better. Take an outside look at each situation and think of why it unfolded the way it did, how it could have unfolded differently, and what can be done next time to improve it.

Notes

1. B.P. McCoy, *The Passion of Command: The Moral Imperative of Leadership,* (Quantico, VA: Marine Corps Association, April 2007).

2. *The Free Dictionary, s.v.,* "proprioception," available at http://medical-dictionary.thefreedictionary.com.

3. Ibid.

4. Daniel Kahneman, *Thinking, Fast and Slow,* (New York, NY: Farrar, Straus, and Giroux, 2011).

5. Carmine Gallo, "In 6 Words, Tiger Woods Reveals How a Champion's Mind Works," *Inc.,* (Sept 2018), available at https://www.inc.com.

6. Headquarters Marine Corps, *MCDP 1-3, Tactics,* (Washington, DC: July 1997).

7. Ibid.

8. Ibid.

9. Christopher Paparone, "Two Faces of Critical Thinking for the Reflective Military Practitioner," *Military Review,* (Fort Leavenworth, KS: November-December 2014).

10. Ibid.

11. Donald A. Schön, *Educating the Reflective Practitioner: Toward a New Design for Teaching and Learning in Professions,* (San Francisco, CA: Jossey-Bass, 1987). Quoted in "Two Faces of Critical Thinking for the Reflective Military Practitioner."

12. Donald A. Schön, *The Reflective Practitioner: How Professionals Think in Action,* (New York, NY: Basic Books, Inc., 1983).

13. Nassim Taleb, *The Black Swan,* (New York, NY: Random House Trade Paperbacks, 2007).

The Big Nine

reviewed by Randy Mieskoski

In her book, *The Big Nine*, author Amy Webb examines the artificial intelligence (AI) component to China's Belt and Road Initiative as a means of soft power. She assesses optimistic, pragmatic, and catastrophic scenarios where the Chinese Communist Party leverages AI as a pathway to attaining its vision for global dominance in economics, geopolitics, and military strength. The book supplements a comprehensive national defense perspective for Marines by exploring potential outcomes of China's ambitious digital strategy.

The Big Nine are U.S. and Chinese technology companies leading AI development. The United States led G-MAFIA consists of Google, Microsoft, Amazon, Facebook, IBM and Apple, while the Chinese leaders are the BAT: Baidu, Alibaba, and Tencent. Webb alternates scenarios between these two groups and explains the potential results on geopolitical world order based on their differing strategies and motivations. Marines building a holistic model of national security threats will better understand how China's massive, government funded AI investments at Chinese universities and the BAT are driving the economic and military advantage China seeks over Western nations. In a fitting analogy, she describes this investment as China's space race, with United States AI as the Sputnik to their Apollo mission.

For Marines not well versed in AI technology, Webb begins with a detailed, historical background of AI and makes a point to define AI versus machine learning. Additionally, she provides astonishing examples of machine learning systems beating chess masters. These systems advanced to "deep learning" AI systems capable of dominating world grandmasters in the complex Chinese board game, "Go."

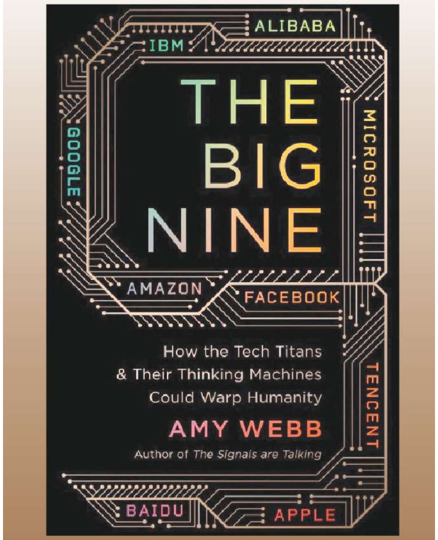
>Mr. Mieskoski is a former 0802 currently working in Civil Service at the Pentagon.

Conjuring up images of the movie *Terminator*, she explains how deep neural net machines will ruthlessly pursue a goal at all costs. Marines will benefit from a cohesive overview of this challenging and ever evolving field to better assess and discuss AI integration into MAGTF applications.

As a quantitative futurist, Webb studies trends to develop data driven scenarios rather than predictions. These models are intended to assist long-term planning decisions. Her optimistic scenario outlines China seeking to gain an absolute advantage over the United States in economic power, geopolitical influence, and military might. However, if the G-MAFIA builds an internal coalition to protect and preserve AI, China will be isolated and find its Belt and Road Initiate in jeopardy as their partners drop out.

Webb argues President Xi Jinping's aggressive national AI strategy for China rivals any unified U.S. approach. However, her pragmatic model infers the BAT could struggle to innovate like Silicon Valley because of the constricting influence of Beijing. This creates opportunities for the DOD's Joint Artificial Intelligence Center to take advantage of AI systems to introduce doubt or poison adversary AI systems to compete against each other.

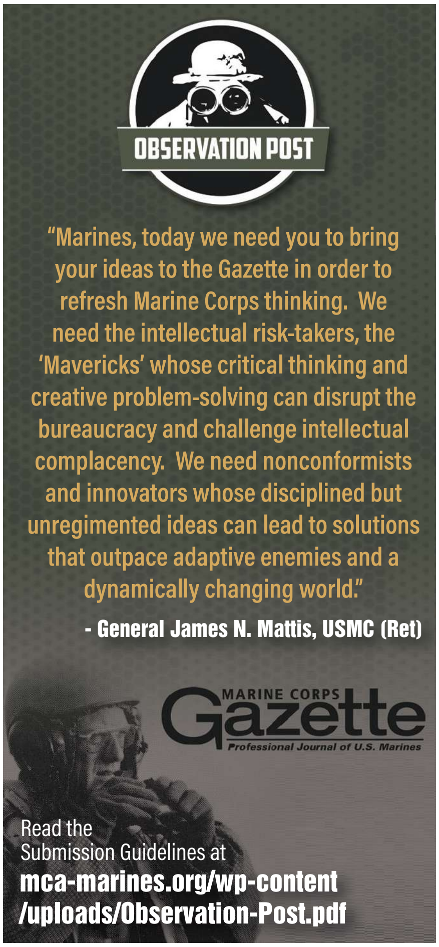
Her catastrophic scenario outlines China's growth as the world's unchallenged hegemon. By exploiting its advantages in key parts of the fifth-generation supply chain and a vast collection of intellectual property, China will expand the Belt and Road Initiate beyond bridges and highways to export AI surveillance technology and isolate the United States. With no privacy or security restrictions, China develops an overwhelming advantage in AIs most precious commodity: data. This AI advantage postures the Chinese Communist Party as the global influencer.


ALIBABA
IBM
GOOGLE
THE BIG NINE
MICROSOFT
AMAZON
FACEBOOK
How the Tech Titans & Their Thinking Machines Could Warp Humanity
TENCENT
AMY WEBB
Author of The Signals are Talking
BAIDU
APPLE

THE BIG NINE: How the Tech Titans & Their Thinking Machines Could Warp Humanity. By Amy Webb. New York, NY: Public Affairs Hachette Book Group, 2019.
ISBN: 978-1-5417-7375-2, 266 pp.

Marines will find this book provides deeper international insight and awareness into China's national strategy and ambitions beyond the four dimensions of national power and the conventional Belt and Road Initiative model. At times, Webb's alarm sounding appears over amplified. However, the book provides alternative viewpoints to the near-peer competition outlined in the 2018 *National Defense Strategy* and is recommended for Marines on a staff assignment at the Pentagon or to current students of PME.

Index to Advertisers


OBSERVATION POST
"Marines, today we need you to bring your ideas to the Gazette in order to refresh Marine Corps thinking. We need the intellectual risk-takers, the 'Mavericks' whose critical thinking and creative problem-solving can disrupt the bureaucracy and challenge intellectual complacency. We need nonconformists and innovators whose disciplined but unregimented ideas can lead to solutions that outpace adaptive enemies and a dynamically changing world."
- General James N. Mattis, USMC (Ret)
MARINE CORPS Gazette
Professional Journal of U.S. Marines
Read the Submission Guidelines at
mca-marines.org/wp-content/uploads/Observation-Post.pdf

Editorial Policy and Writers' Guidelines

Our basic policy is to fulfill the stated purpose of the *Marine Corps Gazette* by providing a forum for open discussion and a free exchange of ideas relating to the U.S. Marine Corps and military and national defense issues, particularly as they affect the Corps.

The Board of Governors of the Marine Corps Association & Foundation has given the authority to approve manuscripts for publication to the editor and the Editorial Advisory Panel. Editorial Advisory Panel members are listed on the *Gazette's* masthead in each issue. The panel, which normally meets as required, represents a cross section of Marines by professional interest, experience, age, rank, and gender. The panel judges all writing contests. A simple majority rules in its decisions. Material submitted for publication is accepted or rejected based on the assessment of the editor. The *Gazette* welcomes material in the following categories:

- Commentary on Published Material: The best commentary can be made at the end of the article on the online version of the *Gazette* at https://www.mca-marines.org/gazette. Comments can also normally appear as letters (see below) 3 months after published material. BE BRIEF.
- Letters: Limit to 300 words or less and DOUBLE SPACE. Email submissions to gazette@mca-marines.org are preferred. As in most magazines, letters to the editor are an important clue as to how well or poorly ideas are being received. Letters are an excellent way to correct factual mistakes, reinforce ideas, outline opposing points of view, identify problems, and suggest factors or important considerations that have been overlooked in previous *Gazette* articles. The best letters are sharply focused on one or two specific points.
- Feature Articles: Normally 2,000 to 5,000 words, dealing with topics of major significance. Manuscripts should be DOUBLE SPACED. Ideas must be backed up by hard facts. Evidence must be presented to support logical conclusions. In the case of articles that criticize, constructive suggestions are sought. Footnotes are not required except for direct quotations, but a list of any source materials used is helpful. Use the *Chicago Manual of Style* for all citations.
- Ideas & Issues: Short articles, normally 750 to 1,500 words. This section can include the full gamut of professional topics so long as treatment of the subject is brief and concise. Again, DOUBLE SPACE all manuscripts.
- Book Reviews: Prefer 300 to 750 words and DOUBLE SPACED. Book reviews should answer the question: "This book is worth a Marine's time to read because…" Please be sure to include the book's author, publisher (including city), year of publication, number of pages, and the cost of the book.

Timeline: We aim to respond to your submission within 45 days; please do not query until that time has passed. If your submission is accepted for publication, please keep in mind that we schedule our line-up four to six months in advance, that we align our subject matter to specific monthly themes, and that we have limited space available. Therefore, it is not possible to provide a specific date of publication. However, we will do our best to publish your article as soon as possible, and the Senior Editor will contact you once your article is slated. If you prefer to have your article published online, please let us know upon its acceptance.

Writing Tips: The best advice is to write the way you speak, and then have someone else read your first draft for clarity. Write to a broad audience: *Gazette* readers are active and veteran Marines of all ranks and friends of the Corps. Start with a thesis statement, and put the main idea up front. Then organize your thoughts and introduce facts and validated assumptions that support (prove) your thesis. Cut out excess words. Short is better than long. Avoid abbreviations and acronyms as much as possible.

Submissions: Authors are encouraged to email articles to gazette@mca-marines.org. Save in Microsoft Word format, DOUBLE SPACED, Times New Roman font, 12 point, and send as an attachment. **Photographs and illustrations must be in high resolution TIFF, JPG, or EPS format (300dpi) and not embedded in the Word Document. Please attach photos and illustrations separately.** (You may indicate in the text of the article where the illustrations are to be placed.) Include the author's full name, mailing address, telephone number, and email addresses—both military and commercial if available. Submissions may also be sent via regular mail. Include your article saved on a CD along with a printed copy. Mail to: *Marine Corps Gazette*, Box 1775, Quantico, VA 22134. Please follow the same instructions for format, photographs, and contact information as above when submitting by mail. Any queries may be directed to the editorial staff by calling 800–336–0291, ext. 180.

I SERVED
FOR my family's safety
YOU ARE NOT FORGOTTEN