MARINE CORPS Gazette
Professional Journal of U.S. Marines

APRIL 2024 Vol. 108 No. 4 www.mca-marines.org/gazette

FOCUS ON INFORMATION

THE MODERN DAY MARINE EXPO: APRIL 30–MAY 2, 2024

A publication of the Marine Corps Association

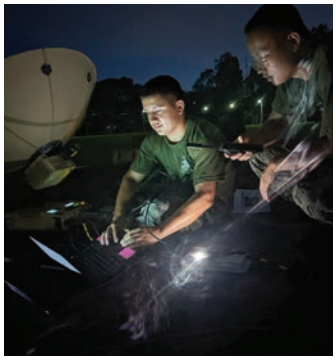
SPIRITUS INVICTUS

THE *UNCONQUERABLE SPIRIT* OF MARINE RAIDERS.

TAKE YOUR PLACE.
TEXT MARSOC TO 87211 // MARSOC.COM

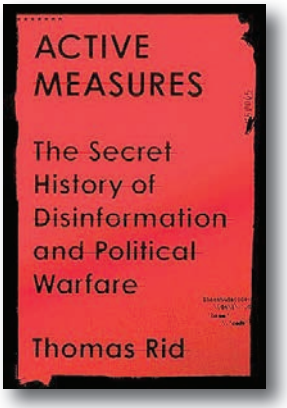
April 2024
Volume 108 Number 4

MARINE CORPS Gazette
Professional Journal of U.S. Marines



62 Cover Article
MCWS-X Night. Marines with 3d MarDiv Communications Company establish a Marine Corps Wideband Satellite Expeditionary terminal as part of an expeditionary communications node. (Photo provided by author.)

DEPARTMENTS



98 Book Review

IDEAS AND ISSUES

Information & C4

PME

Wargaming/Advertiser Content

The *Marine Corps Gazette* (ISSN 0025–3170) is published monthly by the Marine Corps Association 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 • ADVERTISING QUERIES: Contact Valerie Preletz at advertising@mca-marines.org/703–640–0107 or LeeAnn Mitchell, VP Sales at 703–640–0169. • COPYRIGHT 2024 by the Marine Corps Association. All reprint rights reserved. • EDITORIAL/BUSINESS OFFICES: All mail and other queries to Box 1775, Quantico, VA 22134. Phone 703–640–6161. 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 except for such products or services clearly offered under the MCA's name. The publisher reserves the right to accept or reject any advertising order at his absolute discretion.

MARINE CORPS WRITERS

WANTED

TO CHALLENGE THE STATUS QUO AND PROVIDE THEIR INSIGHTS ON RADICAL CHANGE.

THE MAJGEN HAROLD W. CHASE PRIZE ESSAY CONTEST

Submit entries anytime from 1 January to 30 April.

See p. 93 for instructions.

The writing contest is open to active duty Marines and members of the Marine Corps Reserve.

MARINE CORPS ASSOCIATION EST 1913

This content is sponsored by: Observer Media Group Inc.

MARINE CORPS ASSOCIATION
EST 1913

MARINE CORPS Gazette
Professional Journal of U.S. Marines

APRIL 2024

Editorial: Information

A glance at this edition's table of contents shows that our focus this month is on a broad range of topics related to information and the art and science of Marine operations in this complex dynamic environment. Achieving and maintaining competitive advantages from the tactical to the strategic levels in this emergent warfighting function and domain of warfare requires a common vision and careful integration of hardware and software systems, terrestrial and satellite networks, and human talent all underpinned by "TTPs" policies and authorities. While the ubiquity and speed of technological change in the last four decades demand the Corps and the entire defense establishment implement changes to outpace our adversaries and competitors, the importance of information in warfare can be seen as early as Sun Tzu's (Sun Zi's) *Art of War* from the Samuel B. Griffith Translation: "Know the enemy, know yourself; victory will never be endangered. Know the ground, know the weather; your victory will then be total." "All warfare is based on deception." "Let your plans be dark and impenetrable as night." Articles in our focus area begin with a "Message from the Deputy Commandant for Information" by LtGen Matthew G. Glavy on page 6 followed by "Fighting Smart" by LtGen Glavy and Mr. Eric X. Schaner on page 8. This article provides an overview of the Corps' approach to the inter-related systems and human talent required to preserve, deny, project, and protect information. Noteworthy articles focusing on the "art" of information in warfare include "Information in Marine Corps Operations" by LtCol Joseph Uchytil on page 16, "*Warfighting* Through Data-Centricity" by Maj Michael Kennedy on page 20, "Subduing the Enemy Without a Fight?" by 2ndLt Paul Shields on page 40, and "Hacking the Minds of Decision Makers" by Capt Corey A. Ware on page 56. Standout science-focused articles include on page 44 "Hyperscale Cloud Services for Marine Corps Operations" by LtCol Christopher Tsirlis, and on page 66 "Managing CMMC Status Validation for COTS Equipment in Gray Space Acquisitions" by Maj Lawrance Andrus Jr.

Training and developing the human capital required to operate in the information domain are the subject of "Accelerating Cyberspace Talent Development and Readiness" by Mr. Alfredo Rodriguez III on page 24 and "Building All-Domain Communicators" by Maj Adrian Felder, et al. on page 62.

Some may disagree with the Corps' approach, and their fact-based opinions are welcome in the professional journal. No single technology or capability will ever be the sole decisive factor in warfare. However, the pace of change in information is producing changes in the character of war. What began in 1969 with the Advanced Research Project Agency Network and 1983 with the first U.S. analog cellular phone network and civilian access to Global Positioning System satellites, today involves space-based capabilities, artificial intelligence/machine learning, virtual and augmented reality, and a connected video camera in the hands of millions of humans. Absent the right capabilities and a comprehensive understanding of all aspects of information—to include command and control, intelligence, network operations, deception, influence, and controlling a narrative—the risks to the mission and the force increase at the speed of light.

Christopher Woodbridge

Wargaming

Maybe our Corps can be the leader in promoting a change that is long overdue. We use the terms "wargaming," "war gaming," or "war-gaming" as a quick description of the incredibly complex and sophisticated analyses of past and future military conflicts. These analyses are anything but games. They are, for the most part, high-powered computer analyses of myriad possible combat decisions and strategies, in a designated theater of conflict, with the probable conclusions and costs analyzed. They provide relevant guidance that will save lives and capital. They allow our decision makers to test and try innovative and "off the wall" possible military solutions without getting anyone killed and without the cost of "forgetting to pack the band aids" in future conflicts. Maybe we should call them simulations of conflict, "what if" testing, or anything but wargaming. Should MCA offer the renaming as a contest, I will happily buy beer for the winner.

Robert Koury

January 2024

As usual, the January 2024 issue had interesting and thought-provoking articles. I offer some comments.

The "Contaminated Fitness Reports" piece by CWO4 Baldwin should have included reports from other than reporting seniors who were relieved for cause. Some reporting seniors are not up to par in leadership style and traits; these reports should be noted, at least hopefully, by the reporting officer and Headquarters Marine Corps.

The "Officer MOS Assignment System" by 1stLt Houser was very timely. I write this because of the effort or at least discussions of bringing in people without boot camp or Officer Candidate School experience but who possess highly technical or esoteric skills. The lieutenant's last sentence sums it up beautifully.

The overview of "Enhancing Marine Corps Leadership and Readiness" got my keen attention as I served for a commanding general's inspection period as the assistant inspector general for 1st MarDiv. I submitted two recommendations to Headquarters Marine Corps while in the billet. My basic recommendation for both was to design checklists to actually describe the processes that are used day-to-day. If offices make a habit of doing things the way Headquarters Marine Corps wants them done and it becomes routine, all inspections should be "no notice," and more importantly, all organizations should doing things the right way and should be able to pass any inspection.

My favorite article was "Mess Nights" by 1stSgt Kurek, and the subtitle was a bullseye: "A fading tradition." I had to go into my dungeon and pull my literature and old programs here. I would suggest that mess nights (only for members of the mess [and the guests]) are entirely different from dining-ins (spouses and others are invited). One of the most memorable dining-ins I attended was on Camp Butler when our guest was MajGen Day. He gave the most inspiring and *esprit de corps* talks about Marine Corps leadership I ever heard. It centered around his World War II experience and centered on his company commander. We cannot, and should not, lose any more of our culture, heritage, and traditions. That is what makes Marines, Marines.

Lastly, I must comment on what might be a slight to those of us who are currently or previously in the MOS areas of talent management and administration (general and personnel). I just looked (in the dungeon while there) at the October-December issues. The editorial for this month gives the name, title, and page number of the focus articles. The second paragraph continues this, but for those supplementary articles, only a passing notice of what is in the edition. The space seemed available to at least include some of the authors.

It appears that I am still fighting to make sure admin Marines are considered full, real Marines. I was told not to submit a reply back to Manpower Management Officer Assignment when we received a letter that reassigned a 0302 to a 0180 MOS due to the officer's "demonstrated lack of leadership and professionalism."

Needless to say, this characterization of my mentors was not accurate. My senior 0170s and 0180s were mainly former 03s and were of the highest professionals and maintained the highest degree of leadership I had the pleasure to be associated with during my career. The previous year's dining-in, in which a non-admin type proofed the program, let slide "road beef" vice roast beef in the mess night traditions description. Not that big of a deal, but we all have our skills—and all of our skills are necessary and required for the Marine Corps to succeed.

So, I ask that future editorials be reviewed to ensure that, regardless of what the primary focus articles are, the other articles and those writers, whatever MOS they may be, are given the recognition and respect they deserve.

Maj J.H. Thompson (Ret)

Response

No disrespect intended, and I regret the perceived slight. We have so many great articles, and I try to fit as many highlights into my editorial as possible whether they are in the monthly "focus area" or not without re-writing the entire table of contents. In the future, I'll do better recognizing more authors. Semper Fi.

Editor-in-Chief

Updated Bio

In the March 2024 edition, we would like to update Maj Davidhizar's biography for his article, "Don't Make it Complicated." It should have read: Maj Davidhizar, USMCR, is a Logistics Officer and Judge Advocate currently on active duty as an Operational Logistics Planner with MARFOREUR/AF. Maj Davidhizar has deployed to Central America and Afghanistan. His additional MOSs include Foreign Area Officer and Advanced Foreign Security Force Advisor.

Letters of professional interest on any topic are welcomed by the *Gazette*. They should not exceed 300 words and should be DOUBLE SPACED. Letters may be e-mailed to gazette@mca-marines.org. Written letters are generally published three months after the article appeared.

The entire *Gazette* is now online at www.mca-marines.org/gazette.

Garments Below are Approved by NAVAIR

Every design, manufacturing, and sourcing decision that was made to bring our gear to life was done with clear intention. The type of protection that members of SAR communities and our country's armed forces require is unique and challenging. We take pride in the fact that we maintain a tight focus on meeting and exceeding the needs of our end users. From the first NOMEX® fleece suit that Massif®'s founder, Randy Benham, hand sewed in his parents' garage to the cutting-edge new offerings, like our Elements line available this year — every garment was built to protect.

Since we started Massif in 1999, 25 years ago, the number of people using our gear has grown by magnitudes. While the needs that our products address are vast, our mission has remained the same, **Massif®'s passion is to design and create advanced technical apparel that protects the United States Military and those working in the world's most challenging environments.**

Advanced Quarter Zip Combat Shirt (FR)

Hellman Combat Pant (FR)

2-Piece Flight Suit Jacket + Pant — NAVAIR (FR)

ELEMENTS JACKET + Pant — NAVAIR (FR)

Combat Ensemble

CORPORATE HEADQUARTERS

498 Oak Street
Ashland, Oregon 97520

541.488.0801 or 1.888.462.7743
customerservice@massif.com

MASSIF.COM

MASSIFGear
MASSIFGear
MASSIFGear
MASSIFFilms

NEED SUPPORT?

We are here for you.
Please email us at salesteam@massif.com

Corporate information:
CAGE CODE 78EE2, DUNS 079534964

For patent information, please visit MASSIF.COM/PATENTS

MASSIF.COM

100% MADE IN THE USA

BERRY AMENDMENT COMPLIANT

A MESSAGE FROM THE DEPUTY COMMANDANT FOR INFORMATION

When I assumed the role of Deputy Commandant for Information in July 2021, Russia had not yet invaded Ukraine, Hamas had not yet attacked Israel, the Red Sea was unimpeded, and China had not yet rammed Philippine vessels in the South China Sea. These events and China's now frequent crossing of the Taiwan Strait median line highlight just how much the world has changed in recent years. What is at the center of this change? Information—*and the battle to dominate with it*—is transforming the character of warfare. The side that wins the fight for information will most likely succeed in battle and win in war. Just like in the previous decade when we watched "rag tag" violent extremists with up-gun Hilux pick-up trucks, Android 6 smart phones, and commercial VSATs provide formidable challenges in two countries, we again witness the power of data and information in the execution of warfare in asymmetric ways. Peer and non-peer adversaries are increasingly leveraging prolific sensors, data, computing power, artificial intelligence, autonomous systems, and social media to offset historical US military advantages. The Marine Corps is postured to adapt and viciously exploit the power of information to meet these challenges.

Last August General Smith provided me guidance affirming that information plays a major role in supporting his vision for the Marine Corps' continued evolution. Commandant Smith recognizes the fundamental shift in the character of warfare, and most importantly that people, above all else, remain the ultimate source of our Corps' military advantages. Marines empowered by data, information, and cutting-edge technologies, who can also counter the enemy's use of these same things, will advance the Marine Corps as a primary contributor in joint warfighting.

To fulfill the guidance and continue the Marine Corps' evolution in a rapidly changing world, General Smith specifically tasked the DC I team to develop a top-level vision for *information* in the Marine Corps. This task requires us to develop a clear explanation for how data, information, communications, intelligence, cyberspace, space, electromagnetic spectrum, and all other information-based capabilities and functions contribute as an integrated whole to joint competing and warfighting, across domains. This is no small task. To build toward this vision, we must apply what we've learned from the past several years of Force Design to help craft that explanation. Then we must use the vision to drive continued progress in our current phase—Force Development.

In this Gazette issue we take a step toward a top-level vision for information by introducing "Fighting Smart" as the title for the vision, directed by the Commandant. Fighting Smart is the application of our time-tested maneuver warfare principles in our modern hyperconnected world. It is a way of operating that turns data and information into combat power by enabling Marines to make better decisions at a faster pace than the adversary, while using data as an asset that makes all-domain command and control and combined arms faster and more effective. Marines who harness data, information, and intelligence to achieve decision advantage, combine multi-domain effects, close kill webs faster than the adversary, and influence the narrative will achieve advantage in current and future warfare—this is what we seek to achieve through *Fighting Smart*.

Matthew G. Glavy
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Information


Our innovation connects and
protects across all domains.
NORTHROP
GRUMMAN
ngc.com/gator

Fighting Smart

Information in 21st-century competition, deterrence, and warfare

by LtGen Matthew G. Glavy & Mr. Eric X. Schaner

>LtGen Glavy is the Deputy Commandant, Information.

>>Mr. Schaner is a retired Intelligence Officer currently serving as the Deputy Director for the Plans and Strategy Division within the Deputy Commandant for Information.

The character of warfare is changing faster than most could have imagined a decade ago. In just the last four years, Russia invaded Ukraine, Azerbaijan resumed conflict with Armenia, Hamas attacked Israel, Houthis impeded the Red Sea, and China rammed Philippine vessels in the South China Sea. These events and China's now frequent crossing of the Taiwan Strait median line highlight just how much the world has changed in recent years. We observe from these events that the character of warfare is now faster and more connected than ever before.[1] War remains the ultimate contest of human wills and may be long-lasting, but battlefield engagements from sensor to shooter occur faster than ever and are decided quickly by converging multi-domain effects.[2] Kill chains are evolving into complex but resilient kill webs. State and non-state actors are building kill webs by combining readily available capabilities to improve their maturing precision-strike regimes. For state actors, this includes using widely available low-cost sensors, publicly available information, commercially available sensor data, social media, and state-owned sensor data to employ a widening array of precision stand-off weapons, ranging from low-cost unmanned aerial systems and loitering munitions to long range hypersonic and ballistic missiles.

Highly connected technologies such as social media are also fundamentally transforming the battle over narratives. From the conflicts already mentioned to numerous other potential flashpoints in East Asia, opponents in competition and conflict and their supporting public are continually bombarded with messaging through an unending stream of videos, images, and other forms of communication. This messaging is aimed at influencing the enemy to quit, or rival public to acquiesce, or both. What is at the center of all this change?

Information—*and the battle to dominate with it*—is fundamentally transforming the character of warfare. The side that wins both the technical and cognitive fights for information will most likely succeed in battle and win in war. Peer adversaries understand this well. They are leveraging the global proliferation of sensors, abundant data, virtually unlimited computing power, artificial intelligence, social media, and hyperconnectivity to adapt, evolve, and in some cases transform their capabilities to offset historical U.S. military advantages.[3]

... battlefield engagements from sensor to-shooter occur faster than ever ...

The Marine Corps must continue to adapt to meet today's technology-driven challenges in our highly connected world. Marines who harness information to achieve decision advantage, combine multi-domain effects, close kill webs faster than the adversary, and influence the narrative will achieve advantage in current and future warfare. The Marine Corps' adaptation will continue by learning from current events and taking advantage of the opportunities that access to data and information provides. FMFs are doing this today through formations like the MEF Information Group and the Marine littoral regiment, among others. We must do more.

The Commandant's Task to DC I.

In anticipation of these challenges, the Marine Corps created the Deputy Commandant for Information (DC I) position and supporting organization in 2017. The DC I organization brings together the intelligence and information warfighting functions, plus the data and communications functions, into one organization, among other changes.[4] From the beginning through today, the DC I team has worked hard to:

- Develop new doctrine including *MCDP 8, Information*, and *MCWP 8-10, Information in Marine Corps Operations,* to help institutionalize the information warfighting function.
- Establish the Marine Corps Information Command to help Stand-in Forces (SIF) connect with the authorities and permissions they need to operate, as well as leverage intelligence community (IC) capabilities.
- Foster the MEF Information Group's growth from a fledgling operational unit to a fully functional command that can command and control forces across the globe.

- Establish the Network Battalions to secure, operate, and defend the Marine Corps Enterprise Network, providing global support to our MEFs and Marine Forces.
- Create the new 17XX *information maneuver* occupational field by combining cyberspace, space, and numerous legacy information operations fields into a single coherent professionalized series.
- Implement hybrid cloud through network modernization to prepare us for artificial intelligence (AI) enabled data-centric operations.
- Establish the Information Development Institute to provide quality training, education, and experiences for information technology, cyberspace, and the data and AI civilian workforce.

All the above are necessary footings for what is coming next.

In August 2023, Gen Smith provided guidance affirming that information plays a major role in supporting his vision for the Marine Corps' continued evolution. Additionally, Commandant Smith's guidance recognizes the fundamental shift in the character of warfare, and that Marines, above all else, remain at the center. Echoing Col John Boyd's simple but time-tested wisdom of "People, Ideas, Things—in that order," Marines remain our ultimate source of strength and advantage. So long as warfare remains a contest of *human* wills, Boyd's influence on the Marine Corps' warfighting philosophy discussed in *MCDP 1*, *Warfighting*, still drives us to embrace, empower, and trust the creativity and ingenuity of our Marines. Our Commandant and the DC I recognize this and will always put Marines first. We will focus on Marines and enable their creativity by giving them the data, information, and cutting-edge technologies that are available today. Empowering and trusting Marines differentiates us from all our adversaries. It is what gives us a competitive edge. Our duty is to empower and trust Marines with 21st-century capabilities—so that we can fight and win 21st-century battles.

To move us faster in this direction, the Commandant tasked the DC I team to develop a top-level vision for information in the Marine Corps. This task requires us to deliver a unified vision for how data, information, communications, intelligence, cyberspace, space, electromagnetic spectrum, and all other information-based capabilities and functions across the DC I portfolio empower Marines and contribute as an integrated whole to joint warfighting. This is no small task. To build this vision we must apply what we learned over the past several years of Force Design to help drive the next phase—*force development*.

What Have We Learned So Far?

The Marine Corps is transitioning from a simpler view of the battlespace organized around physical maneuver combined with supporting arms to a more sophisticated view of all-domain combined arms. While we have made great progress in this transition in recent years, trend reporting from our MAGTF Warfighting Exercises shows we have more to do.[5] The core challenge we face is how to create and sustain the ability to close complex kill webs while preventing our adversaries from closing them on us. To meet that challenge, we must help Marines understand the role of information and how to use data to enable and support that effort. Another primary challenge is helping Marines understand they are always in a narrative battle and giving them the tools they need to successfully fight that battle. These are information problems that we can and will solve.

To achieve the above, the Marine Corps must solve several human capital issues. Putting Boyd's philosophy of "People, Ideas, and Things—in that order" into practice, we must first address an all-Marine education and training issue. Every Marine, especially commanders, must better understand their role in data-centric operations and how to integrate and exploit information across warfighting functions. Next, the Marine Corps must fix problems related to the development and retention of Marines and civilians serving in the information-related fields. These problems range from lack of specialization in essential high-demand, low-density skills to career stagnation and inefficient utilization. Additionally, the Marine Corps must overcome similar problems in producing and retaining sufficient personnel in the intelligence occupational fields.

The Marine Corps is not maximizing the use of data to empower people and help them make decisions. While data is at the root of all Marine Corps functions, missions, and activities, the Marine Corps' data is not currently organized, structured, governed, processed, and presented in a way that allows for effective use or decision making. This suboptimal use of data puts Marines in a situation of seeking information-based advantages through constant trade-offs among data, intelligence, and communications needs. Until such time as we finally synchronize "information" into a single unifying concept that integrates these areas along with cyber and space, the Marine Corps will continue to fall short.

With respect to intelligence, the findings of force design-related analysis, wargames, and exercises match observations of the contemporary operating environment: winning the reconnaissance and counter-reconnaissance (RXR) fight is critical. The Marine Corps Intelligence, Surveillance, Reconnaissance Enterprise (MCISR-E) must continue to modernize to anticipate and stay ahead of changes in the environment to enable Marines to win the RXR fight as part of joint competing and warfighting. The MCISR-E must incorporate the use of data and information technologies that enable rapid sense-making of large, multi-disciplinary data sets and intelligence feeds, as well as software-defined two-way connectivity across the Marine Corps and to the Joint Force and IC.

In a highly connected two-way data-centric environment the exquisite capabilities of the IC are instantly available, globally. The findings show a need to leverage this connectivity to enable SIF to not only be the eyes and ears of the Joint Force but also the IC. In response to this need, the Marine Corps established the Marine Corps Information Command to tie the SIF closer to the IC and global combatant commanders like

CYBERCOM and SPACECOM. This connection crucially enables mutually supporting relationships between the SIF and combatant commanders—allowing for the exchange of data, authorities, and permissions, as well as using placement and access to generate effects.

We have learned a great deal from current events and the Marine Corps' collective campaign of learning. We must now capitalize on what we have learned to continue improving.

Toward a Unified Vision for Information.

The diverse functions and capabilities within the DC I portfolio exist to help Marines and the Marine Corps gain or exploit some kind of information-based advantage or effect. The Commandant's task to create a unified vision for information is a task to help him organize, train, and equip the Marine Corps to harness the power of information and technology for the purpose of gaining and exploiting information-based advantages and effects. This is the basis for "fighting smart" as a unified vision—a vision that draws directly from the last sentences of *MCDP 1*, *Warfighting*, which state: "Maneuver warfare is a way of thinking in and about war that should shape our every action ... [it] is a philosophy for generating the greatest decisive effect against the enemy at the least possible cost to ourselves—a philosophy for 'fighting smart.'"[6]

How do Marines fight smart in the 21st century? How do Marines develop insight, leverage their imagination, and innovate to adapt to disruptive environments? How does the institution deliver cutting-edge technologies to turn data and information into tactical advantages and combat power? How do Marines use these advantages to out-*think*, out-*compete*, and out-*fight* the adversary? These are some of the fundamental questions Fighting Smart will answer.

To build toward this vision and answer these fundamental questions, the Marine Corps must close gaps associated with the Commandant's priorities of *people*, *readiness*, and *modernization*. Concerning people and readiness, we must educate and train individual Marines to know what to do with information and their role in using it effectively, and then match people to billets to take maximum advantage of their skills and available technologies. This includes integrating individual talent into realistic and challenging unit training. This combination enables a data-centric approach to operations. Commanders and Marines at all levels benefit from their ability to make better and faster decisions than the adversary, and their ability to manipulate or deny information to the adversary in ways that maintain or increase warfighting advantages.

With respect to modernization, we must improve our ability to combine all available data using advanced technologies to move relevant and trusted information in a timely manner—this makes distributed operations possible, as well as all domain RXR through a modernized MCISR-E. Additionally, combining all available data enables ally, partner, and Joint Force integration into all-domain combined arms to close joint and combined kill webs, which greatly increases the potential dilemmas Marines can create for their adversaries. To accomplish this, the Marine Corps must develop an organizing concept and formations that integrate signals intelligence, electromagnetic spectrum operations, and cyberspace operations.

To leverage data for battlefield advantages, the Marine Corps must learn from current events where adaptability through rapidly engineering software applications and data solutions at the point of need has proved advantageous. The 18th Airborne Corps provides a prime example, demonstrating the effectiveness of deploying a skilled team of software coders and engineers to dynamically create data solutions that support evolving missions and the commander's need for information. Our MEF commanders should possess similar capabilities.

Toward a Fighting Smart Institution

Service leaders and staff can also fight smart by modernizing to support institutional operations. Leaders and staff at all levels benefit from their ability to organize, structure, govern, and process data in ways that allow for effective use and decision making. Modernizing data-centric operations at the institutional level would greatly improve institutional planning; force design and development; acquisition; budgeting; recruiting and retention; assignments; training and education; force generation and employment; posture decisions; strategic communication, and installations and logistics planning.

Fighting Smart applies to all Marines, emphasizing the instant and interconnected global nature of the information environment.

Fighting Smart applies to all Marines, emphasizing the instant and interconnected global nature of the information environment. It underscores the visibility and potential consequences of actions and words by all, including civilian Marines and support contractors. Achieving a unified information vision necessitates practicing information discipline—maintaining professionalism and awareness that every word and action is visible globally. This recognition can either enhance or hinder the Marine Corps' reputational narrative, affecting public perceptions both domestically and internationally.[7]

To continue the Marine Corps' evolution, we must also implement changes to how we conduct defense acquisitions. Marines recognize the need to go faster, with operational commanders using O&M dollars to acquire capabilities. External leaders and Congress have long called for changes. Marine Corps Sys-

Liberty Global Logistics LLC

A Leading Ocean Shipping & Logistics Company

Supporting Marines and Deployed U.S. Forces Globally

tems Command recently reorganized to enhance acquisitions, but more work remains. The Commission on Defense Innovation and Adoption, in its January 2024 publication, underscores the urgent need to swiftly adopt cutting-edge technologies from commercial and defense sectors. Doing so will enable the timelier delivery of high-impact solutions to the warfighter.[8]

This necessitates a fundamental shift in focus within our programs of record to emphasize software requirements over hardware. This shift also requires our programs to allow for rapid software modifications and updates to ensure our warfighters can maintain a competitive advantage by fusing and correlating data to drive decisions, actions, and outcomes. Organizations like the Marine Corps Software Factory are designed to support and enable rapid software development. Fighting Smart will identify necessary actions to steer the Marine Corps toward crucial reforms in requirements development and acquisitions, as well as in providing software development support to FMF.

Where Are We Headed?

Fighting Smart is a way of operating that turns data and information into combat power by enabling Marines to make better decisions at a faster pace than their adversary while using data as an asset that makes all-domain command and control and combined arms more effective. To take full advantage of this operating method, the Marine Corps needs to educate and train its people in how to create and sustain it. Every operating approach relies on skilled people to make it work—Fighting Smart is no different. Marines must know how to get the most from data to make it effective.

Fighting Smart will look familiar to most Marines. It will read like other major Service-level initiatives (e.g., talent management) that were developed over the last several years. However, a key difference is that Fighting Smart will relate to and enable these other initiatives, especially the Commandant's three major priorities mentioned above. Additionally, Fighting Smart will establish directed actions and areas requiring further study within specific focus areas. In the current draft, these areas include mobilizing talent, achieving data-centricity, modernizing the MCISR-E, and enabling 21st-century combined arms. Fighting Smart is expected to be published in June 2024.

Conclusion

Fighting Smart represents an expanding opportunity for 21st-century combined arms, extending beyond traditional domains to include space, cyberspace, the electromagnetic spectrum, and the information environment. It embodies converging effects from multiple domains to drive advantages and outcomes. Taking Boyd's philosophy to heart, people and their ideas, empowered by data and technology, are at the center of Fighting Smart.

People empowered by data are also central to modernizing the MC-ISRE.

It is Marines, not technology, who will ultimately maintain the Marine Corps' competitive edge. Future success demands data-literate training, including AI/ML training within applicable areas of the Marine Corps. Fleet Marine Forces and the supporting establishment require a workforce with specialized skillsets for improved decision making.

People empowered by data are also central to modernizing the MCISR-E. Modernization and Joint Force relevancy require the Marine Corps to function as an RXR force in both competition and conflict, engaging in a daily fight for information and influence. Modernizing the MCISR-E is essential to help close kill webs, which makes 21st-century combined arms possible. A modernized MCISRE also helps create decision advantage and Joint Force resiliency as well as supports understanding and competing in the battle for narratives.

Achieving the above hinges on empowering people with data, providing necessary education and training, and enhancing the institution's speed in delivering data-centric capabilities. Fighting Smart serves as a blueprint for the Marine Corps' evolution in the technology-driven, highly connected world, addressing the need for organizational adaptability to meet modern challenges and reduce the warfighter's operational risks.

Notes

1. John Antal, "The First War Won Primarily with Unmanned Systems, Ten Lessons from the Ngorno-Krabakh War," *Madscriblog,* April 1, 2021, https://madsciblog.tradoc.army.mil/317-top-attack-lessons-learned-from-the-second-nagorno-karabakh-war.

2. Ibid.

3. National Security Commission on Artificial Intelligence, *Final Report: National Security Commission on Artificial Intelligence*, (Washington, DC: 2021).

4. Headquarters Marine Corps, *Marine Corps Bulletin 5400, Establishment of the Deputy Commandant for Information,* (Washington, DC: 2017).

5. Marine Air Ground Task Force Training Command, Marine Air Ground Combat Center, *Final Exercise Report for MAGTF Warfighting Exercise 2-23*, (Twentynine Palms: 2023).

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

7. Headquarters Marine Corps, *MCDP 8, Information*, (Washington, DC: 2022).

8. Atlantic Council, Scowcroft Center for Strategy and Security, *Commission on Defense Innovation and Adoption, Final Report*, (Washington, DC: 2024).


MQ-9B SeaGuardian®
UNMANNED & UNMATCHED
ADVANTAGE AT SEA
MQ-9B SeaGuardian is the future of unmanned aircraft systems today. With industry-leading endurance, superior multi-mission payloads, and assured global interoperability, SeaGuardian is the ideal all-weather, all-domain force multiplier.
Scan to learn more
©2024 GENERAL ATOMICS AERONAUTICAL SYSTEMS, INC.
ISR
24/7
Enabling Information Dominance
GENERAL ATOMICS AERONAUTICAL

Continuous Authorization

Maintaining cyber readiness

by Mr. William Bush

>Mr. Bush is a retired Marine Corps Cyber Network Operations Engineer Officer. He is currently the Deputy Director for the Cybersecurity and Compliance Branch and Authorizing Official Designated Representative, Deputy Commandant for Information.

Risk management framework, also referred to as RMF, is the systematic process of identifying, assessing, and mitigating threats that can affect an organization and its business practices. RMF involves analyzing a risk's likelihood and impact, developing strategies to minimize harm, and monitoring a measure's effectiveness. The Marine Corps currently implements RMF per *National Institute of Standards and Technology 800.53* in managing the cybersecurity risk posed by potential enemies. RMF is a federally mandated process that all DOD organizations must comply with. The RMF process, as currently practiced by the Marine Corps, is a labor-intensive activity, conducted independent of system development. As it consumes an outsized portion of program and supporting organization resources (i.e., subject-matter experts, time, and money), it struggles to enable program offices and organizations to keep pace with the need to innovate and produce mission-relevant capabilities. This article will discuss the direction the Deputy Commandant for Information, Command, Control, Communications, and Computers is heading as we look to modernize the RMF process, thus providing the Marine Corps with an alternative to the current RMF construct.

Change the Way We Do Business

The current implementation of the RMF is labor-intensive and time-consuming, and it does not provide actual cybersecurity risk to the Marine Corps Enterprise Network (MCEN). To be able to deliver cybersecurity measures in realtime to systems and applications, the Marine Corps must move toward a cybersecurity assessment and system authorization model focusing on continuously addressing threats, in turn improving our cyber resiliency. Currently, program managers/system owners are singularly focused on obtaining authorities to operate, which has turned the assessment and authorization process into a checklist of activities that must be accomplished, vice providing a system owner with the actual cyber risk posed to the system and the MCEN.

Continuous authorization moves away from the control assessment point-in-time document-based approach toward focusing on continuous risk determination and authorization through assessing, monitoring, and risk management. Continuous Authorization is centered around the successful employment of continuous monitoring (CONMON), development security operations (DevSecOps), and active cyber defense measures. The implementation of CONMON, DevSecOps, and active cyber defense into our MCEN ecosystem and the larger DOD network environment is imperative to our warfighters as the cyberspace domain is constantly changing and evolving. Moving toward a CONMON model will allow system owners to address old vulnerabilities, as well as track newer threats. CONMON provides operational commanders, system owners, and the authorizing official (AO) with near realtime critical system vulnerability information to support network risk-based decisions. Another major change to the environment is the Marine Corps moving away from being hardware-dependent to a more software-centric environment, where information and collaboration will now take place in the Cloud. DevSecOps is the piece that will ensure secure software development best practices are being used to maintain secure baselines. An active cyber defense model, allows program managers to conduct simulated adversarial assessments on their systems, providing key feedback to potential vulnerabilities based on current threats. This model would allow the Marine Corps to focus financial and personnel resources on the areas required. It is imperative we provide our warfighters with cyber-ready systems and applications at a moment's notice, so the implementation of continuous authorizations in the Marine Corps is the only realistic way ahead.

What Are the Current RMF Process Challenges?

The ability of the current RMF

process to effectively indicate a system's state of cybersecurity protections or readiness is sometimes questioned by stakeholders across the MCEN. As an example, current programs of record are individually assessed through an antiquated stove-piped assessment and authorization process, where the primary objective is to receive an authorization/authority to operate. That cycle is then repeated in three years. Marines have always prided themselves on being more proactive than reactive, but left uncorrected, actions here imply we are willing to accept less from our cybersecurity process. The less-than-effective perception of the RMF process is attributed to issues such as lack of funding, insufficient resources, or the lack of experience within our workforce. As Marines, we have always achieved more in the face of adversity, and we will not change now. However, as cyber threat actors become increasingly prevalent and the techniques and tools they employ become more advanced, our systems and networks must continuously build resiliency to address these threats. Lastly, we have made little progress over the last six years in automating the current RMF process within the Marine Corps, which has made it difficult to keep pace with our adversaries' technological advancements. A combination of all these issues will continue putting our warfighters at risk, so the Marine Corps must address these challenges head-on.

Addressing Continuous Authorization in the Marine Corps

Continuous authorization provides a construct to address those challenges by authorizing and assessing systems throughout the system development lifecycle and alleviates the risk of assessing the cyber status of a system just once every three years. To accomplish continuous authorization, the Marine Corps will continue working efforts alongside the Department of the Navy Chief Information Officer and Navy N2N6 as a member of the Cyber Ready working group, defining how we will implement continuous authorization for persistent and non-persistent systems in the Naval Service. Based on deliverables from the Cyber Ready working group, the Deputy Commandant for Information, Command, Control, Communications, and Computers plans to develop policy and provide guidance in the form of enterprise cybersecurity manuals to assist program managers and systems owners with the transition to a sustainable continuous authorization model. In those enterprise cybersecurity manuals and subsequent policies to follow, we will standardize CONMON processes, tools, and techniques, enabling more reliable cybersecurity assessments of our systems and network. We will also focus on providing more readily available "software factories" for software developers, ensuring DevSecOps is rooted throughout development and deployment, as this will play a large part in providing warfighters with secure applications. Improving the RMF process presents program managers/system owners with an improved way to deter threats and allows for more efficient use of resources in their efforts to keep pace with innovation and new capability development.

Lastly, as the Marine Corps moves toward continuous authorizations, we all need to keep in mind that having a properly trained the right workforce in place will be one of the most important pieces in getting this done correctly. We must not simply focus on cybersecurity personnel but ensure we account for program managers, engineers, and contract officers—as they will be key to the overall success.

USMC

Information in Marine Corps Operations

Information and the changing character of warfare

by LtCol Joseph Uchytil (Ret)

Critical Imperative or Call to Action

The Marine Corps needs a pragmatic reference for operating in and through the information environment. A 2021 RAND study identified that the Chinese People's Liberation Army views information as a key enabler for success in a future conflict and the single most critical domain for success in contemporary and especially next-generation warfare.[1] Leveraging this observation, the *2022 National Defense Strategy* calls for a future force that is resilient—in that it maintains information and decision advantages, preserves command, control, and communications systems, and ensures critical detection and targeting operations. Additionally, the *National Defense Strategy* calls for a department that will improve the Nation's ability to integrate, defend, and reconstitute surveillance and decision systems to achieve warfighting objectives, particularly in the space domain, and despite the adversary's means of interference or deception.[2] These are no small tasks in this age of advancing technology where competitors capitalize on technology and information activities to achieve objectives. While accomplishing these endeavors will require the DOD to examine the challenges across the entirety of the doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy framework to realize success, this discussion is focused on the influence of Marine Corps doctrine to realize these imperatives.

The Marine Corps is moving forward with generating doctrine that presents a path to achieving information advantages through the *MCWP 8-10, Information in Marine Corps Operations*. The June 2023 *Force Design 2030 Annual Update* identified that as the pace of change in the information domain accelerates, the Marine Corps cannot afford to allow doctrinal efforts to languish. It must keep pace with the emerging and evolving operational environment, as well as with the agencies and organizations that will be essential to its success.[3] In support of this analysis, the Deputy Commandant for Information published its second "8" series doctrinal publication. This article will discuss the imperative for the *MCWP 8-10* and review some key topics presented by the publication.

>Mr. Uchytil is currently a defense contractor for Troika Solutions and provides support to the Information Plans and Strategy Division, Deputy Commandant for Information, Headquarters Marine Corps. He served a combined 26 years as both a Marine Corps Communications Officer and enlisted Marine Infantryman.

"While dependent on the laws of science and the intuition and creativity of art, war takes its fundamental character from the dynamic of human interaction."

"War is both timeless and ever changing. While the basic nature of war is constant, the means and methods we use evolve continuously. ... One 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 both to maximize our own capabilities and to counteract our enemy's."

—MCDP 1, Warfighting

Changing Landscape

Leveraging information power is nothing new to the Marine Corps. However, today's hyper-connected digital environment has created new and constantly evolving opportunities and challenges that impact Service and

"Every action a Marine Corps unit or individual Marine takes or does not take has the potential to communicate a message."

—MCDP 8-10, Information in Marine Corps Operations

Joint Force operations from competition to conflict. This current environment poses challenges at all levels of command while simultaneously driving change across the Marine Corps and the greater Joint Force. Commanders across the Service are integrating information considerations into planning efforts and operations to generate multi-domain effects and achieve mission objectives. The speed and reach of today's technology portend that tactical actions can have far-reaching, strategic information and influence implications. Both the accessibility and use of information can be a vulnerability as Marines can quickly upload digital imagery, videos, or other material that has not been appropriately vetted for release and share it on information technology platforms (social media, email, etc.) at the speed of the internet and at the cost of negating command narratives or blunting operational security actions. Recently, MajGen Ryan Heritage, the Commanding General of Marine Corps Forces Cyberspace Command and Marine Corps Forces Space Command, was asked about information and Marine Corps culture. He was quoted as saying, "I would tie that to the Marine ethos, Marine culture, and understanding how information is a key to warfighting and therefore every Marine a rifleman, every Marine needs to understand the power of information and where that's applied and how they apply it."[4] With this in mind, *MCWP 8-10* seizes the opportunity to address how all Marines can apply informational power by presenting innovative solutions to operational problems and strategic challenges within the information environment.

Marine Corps Doctrinal Publication 8, Information

In June of 2022, the Marine Corps published *MCDP 8, Information*. With *MCDP 8,* the Marine Corps established its first Service-level information doctrine. This publication provided a foundational theory for leveraging the power of information, described the Marine Corps information warfighting function, and discussed the function's mutually supporting relationship with other Marine Corps warfighting functions. *MCDP 8's* framework supports the high-level understanding of the Marine Corps information warfighting function and introduces the three information advantages generated through its application: systems overmatch, prevailing narrative, and force resiliency. This foundational doctrine provides the context and theoretical framework that is expanded upon through the *MCWP 8-10. MCDP 8* was written with an understanding of the continuously evolving global security environment and it allows for future subordinate doctrine to keep pace.

Operationalizing *MCDP 8*

MCWP 8-10 is a subordinate publication to *MCDP 8. MCWP 8-10* supports the understanding and employment of the means for conducting information and how those activities generate an information advantage. It operationalizes the information warfighting function and tenets of *MCDP 8* while serving as an intermediary doctrinal publication bridging the gap between the MCDP and the more detailed tactics, techniques, and procedures found in reference or tactical publications. It addresses a methodology for incorporating the four functions of information (generate, preserve, deny, project) and by extension, the information warfighting function into plans, operations, and day-to-day activities. Lastly, it presents principles for assessing successful outcomes and tools to support planners and operators alike in assessing if those activities generated the desired effects. As doctrine is authoritative and not directive, the *MCWP 8-10* requires prudent judgment in its application. It is intended to provide a practical reference for all Marines to leverage the power of information to gain and maintain advantages across the spectrum of operations and activities. Additionally, it seeks to facilitate formal school programs of instruction and unit standard operating procedures to maximize the effectiveness of information activities.

General Information Activities ... Presence, Posture, and Profile

A key tenet of the *MCWP 8-10* is the idea that creating and maintaining information advantages are not solely the responsibility of commanders and staff but rather the total force. *MCWP 8-10* identifies that all operations and activities include inherent informational aspects that must be understood, synchronized, and leveraged as an integral part of planning and operations and that all observed Marine activities can be considered consistent, inconsistent, irrelevant, or contradictory to a prevailing narrative.[5] With this in mind, all Marines would benefit from recognizing the important role that their everyday activities, whether deployed or at their home station, play in the greater context of creating or degrading a friendly information advantage. Every action, from the mundane to the worldly, is an observable activity that communicates a message. Though not specifically stated, *MCWP 8-10* conveys the idea that while it is incumbent upon leaders to ensure Marines understand the prevailing narrative, command messaging, and desired outcomes, the responsibility to ensure actions are consistent with these outcomes resides with the individual Marine.

Both individual and unit actions leverage presence, posture, and profile to convey tactical, operational, and strategic messages. These messages may influence adversary actions or strengthen

... MCWP 8-10 seizes the opportunity to address how all Marines can apply informational power by presenting innovative solutions to operational problems and strategic challenges ...

relationships with friendly forces to achieve an information advantage. Presence, posture, and profile can be visualized in the following ways. *Presence* may be the physical act of being in a location or a virtual space (such as social media and Internet platforms). *Posture* may be how one presents oneself through attitude, stance, comportment, etc. Finally, *profile* is the representative combination of presence and profile to communicate a message to adversaries and friendly forces alike. Conveying consistent, sound, and well-planned presence, posture, and profile helps to shape an operational environment that is advantageous to friendly forces and provides commanders with operational flexibility.

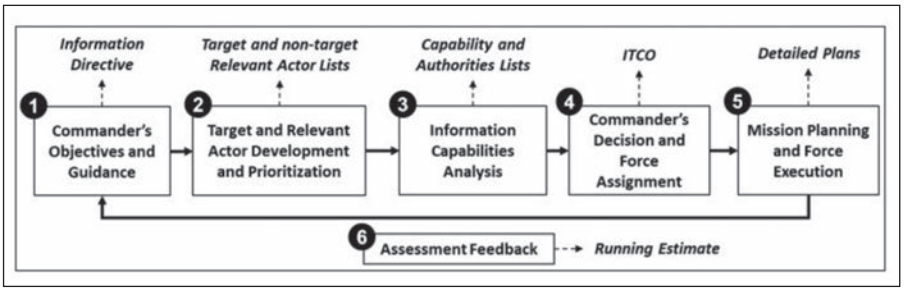


Figure 1. Six ITCC Phases.[6] ***(Figure provided by author.)***

An Objective is ...	*If ...*
Specific	It is well defined and unambiguous and describes exactly what is expected
Measurable	One can measure the degree to which the objectives is being met
Achievable	It is realistic and attainable
Relevant	The achievement of the objective contributes to progress toward high-level strategic and policy goals
Time-Bound	It has deadlines or is grounded within a deadline

Figure 2.[7] ***(Figure provided by author.)***

Planning for Information: Information Tasking and Coordination Cycle and the Information Tasking Order

A hallmark of the *MCWP 8-10* is the introduction of the Information Tasking and Coordinating Cycle (ITCC) and its output, the Information Tasking and Coordinating Order (ITCO). This is the first instance of a doctrinal Marine Corps process for integrating the employment and coordination of specialized information activities and capabilities that predominantly reside in units such as the MEF Information Groups. It establishes a predictable framework for planning, executing, and assessing information activities. Through a six-phase cycle, the ITCC supports the identification of objectives and outcomes; identifies the targets and relevant actors for action; evaluates information activities or capabilities available to achieve the objectives; generates an order for the execution of information activities and tasks; allows for detailed tactical-level planning, coordination, and execution; and identifies the necessity for assessing the effectiveness of the cycle to achieve the objectives. This cycle's products, specifically the ITCO, become the commander's mechanism to synchronize information activities with other communities' cycles, such as aviation, logistics, fires, and maneuver.

The ITCO is the primary product of the ITCC. It conveys all aspects of the ITCC in a product that is approved by the MEF commander. The ITCC is generally understood to be an MEF-level process. However, it can be scaled to apply at any echelon of the organization to facilitate coordination, planning, and execution of specialized information activities to achieve overall operational objectives. While the ITCO identifies those activities of an operations order (situation, mission, execution, admin and logistics and command, and control), the focal point is conveyed through the identification of information tasks. It is through these tasks that the phases of the ITCC are captured and applied to organizations and units. The execution of these tasks along with the effects and outcomes then leads to the ability to assess results and validate if desired effects were achieved.

This cycle's products ... become the commander's mechanism to synchronize information activities with other communities' cycles, such as aviation, logistics, fires, and maneuver.

Assessing the Effectiveness of Information Activities

MCWP 8-10 addresses one of the more difficult activities when discussing information advantage—how to assess whether actions in and through the information environment are achieving the desired outcomes or effects. Rather than an assessment methodology, *MCWP 8-10* presents guiding principles that should be addressed in phase six of the ITCC, emphasizing the necessity to integrate information activities and outcomes into the planning process. Evaluating effects against relevant actor perceptions, behavior, and capabilities is seemingly more challenging than conducting a battle damage assessment of the effects of conventional fires. As such, it is imperative to identify specific, measurable, achievable, relevant, and time-bound (SMART) objectives while executing the first two phases of the ITCC. Objectives generated in phase one or phase two of the ITCC that inadequately ad-

dress SMART criteria will lead to difficulty during phase three when planners identify capabilities to match against relevant actors and desired effects. The *MCWP 8-10* suggests that when objectives follow SMART criteria for assessing effectiveness they directly lead to more valuable measures of effectiveness and measures of performance.

Conclusion

The ever-changing character of warfare requires new approaches to leverage the power of information. Gaining and maintaining an information advantage supports the other warfighting functions and Marine Corps and Joint Force operations as a whole. It accelerates the friendly command and control process to out-cycle the adversary. This translates into making quicker, more informed decisions thus increasing friendly tempo while degrading the adversary's. *MCWP 8-10* expands upon the tenets of *MCDP 8* and provides Marines at all echelons of command the reference material to gain and maintain an information advantage through a practical, repeatable, and predictable framework. It delivers a functional publication for commanders, individual Marines, planners, and staff alike to leverage during planning and operations. It seeks to lay a foundation for the preparation, execution, and evaluation of all information activities thus increasing the options available to commanders in both competition and conflict. The publication of the *MCWP 8-10,* coupled with the *MCDP 8,* delivers a deliberate methodology for integrating information into all facets of warfighting to arm Marines for the challenges of current and future battlefields.

Notes

1. Scott W. Harold, Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung, *Chinese Disinformation Efforts on Social Media* (Santa Monica: RAND Corporation, 2021).

2. Department of Defense, *2022 National Defense Strategy,* (Washington, DC: 2022).

3. Headquarters United States Marine Corps, *Force Design 2030: Annual Update,* (Washington, DC: 2023).

4. Mark Pomerleau, "Marine Corps' New Information Command Needs a Common Operational Picture for Digital Landscape," *Defensescoop*, January 5, 2024, https://defensescoop.com/2024/01/05/marine-corps-information-command-needs-common-operational-picture-digital-landscape.

5. Headquarters Marine Corps, *MCWP 8-10, Information in Marine Corps Operations,* (Washington, DC: 2024).

6. *MCWP 8-10, Information in Marine Corps Operations.*

7. Ibid.

Warfighting Through Data-Centricity

Outmaneuvering through Information

by Maj Michael Kennedy

Information is a critical element of all military operations. This should not surprise us as our observe, orient, decide, and act (OODA) loops are fed by, make sense of, and inevitably generate information. Data is the fundamental building block of information, and one can increase the value of that data by adding additional context or fusing it with other data to convey a greater meaning to the viewer. For example, to an aviator, individual pieces of data such as airspeed, altitude, heading, and navigational data are all important for any given mission, and they can be fused to convey more information via a heads-up display. With this rudimentary data analysis and display, a heads-up display can accelerate an aviator's OODA loop by conveying the needed data in one location, integrated with mission-specific alerts, which provides them with an information advantage. As described in *MCDP 8, Information*, using the right information can create decision, temporal, spatial, and other information advantages that can allow friendly forces to outmaneuver an adversary, which is vital based on the threats posed by peer adversaries.[1]

One of the greatest challenges on the modern battlefield is the time compression introduced by long-range, high-speed weapons and their ability to hold U.S. assets at risk.[2] This sentiment of Wayne Hughes echoes throughout recent Marine Corps publications, including *Force Design* and *A Concept for Stand-in Forces*. The anticipated character of this future conflict necessitates the ability to rapidly observe, orient, and decide so the necessary actions can be taken within the time constraints introduced by enemy weapons. The longer any one of these processes takes, the longer it will take to complete an OODA cycle, which increases the difficulty of gaining a decision advantage.

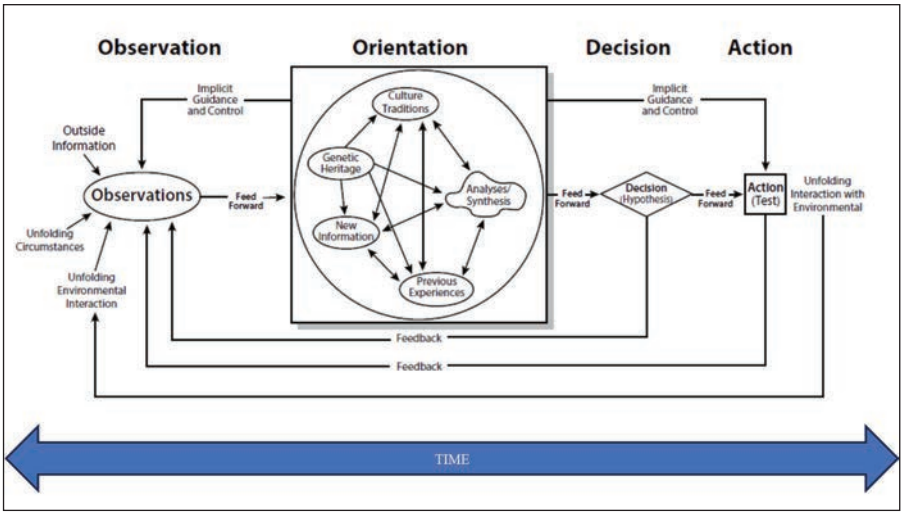


Figure 1. Boyd's OODA Loop with a time component.[3] ***(Figure provided by author.)***

>Mr. Rodriguez is a former Army Lieutenant Colonel and is currently the Information Technology and Cybersecurity Community of Interest Manager. He is the Senior Advisor to the Deputy Commandant for Information Workforce Senior Executive and the Deputy C4/CIO Director. His experience ranges from battalion command to service on multiple echelons across the Army, Joint, and special operations organizations.

The interrelationship between observation and orientation is critical in managing the time required to complete OODA cycles. If the data observed by a Marine is not managed in some way, the sheer amount of available data in a given situation, whether relevant or not, will slow the orientation phase because the Marine must discern what is and is not relevant and then attempt to make sense of what is deemed relevant. If instead the observed information was curated and formatted based on the needs of the Marine, the time taken by observation and orientation could shrink dramatically.

Friction, uncertainty, and complexity also tend to slow this process, and while this fog of war will never abate, it may be possible to lift some of the fog. If Marines can maintain access to relevant and trustworthy data, formatted on mission-specific displays it can provide the opportunity for continued situational awareness and lift some of the fog.

To succeed within this anticipated character of war requires technical change in our systems as well as operational changes in how we generate,

share, and utilize that data to achieve the desired benefits in competition and conflict. The innovation required to achieve a faster relative tempo than our adversaries reside in the idea of data-centricity. This article first describes data-centricity and what it means to the Marine Corps from a doctrinal perspective. After making the linkage to doctrine, the article concludes with ways to implement data-centricity and some examples of what operational benefits could be gained. Please note that many of the examples provided are aspirational to show what is in the realm of the possible. Additionally, I intentionally use vague terms at times so Marines of every MOS can connect these thoughts to the systems they use to complete their mission.

What Is Data-Centricity?

The definition of data-centricity utilized by the DOD is "an architectural approach that results in a secure environment separating data from applications and making data available to a broad range of tools and analytics within and across security domains for enrichment and discovery."[4] In simple terms, this means that individual networks or information systems are *enablers* instead of the main effort. For example, GCSS-MC, M-SHARP, and NALCOMIS OOMA still play a critical role in data generation and storage; however, perhaps a greater value is when that data is fused and analyzed between systems and used to formulate decisions. Perhaps the data in each of those systems could contribute to a model that would reduce the time required to fulfill aircraft parts orders.

This approach enables Marines to utilize all useful data, regardless of system, to facilitate every warfighting function and solve operational problems. A Marine would need access to myriad systems if they wanted specific information pertaining to command and control, fires, force protection, information, intelligence, logistics, and maneuver for a given mission. In a data-centric framework, where the concern is providing access to data in these areas, Marines at all levels can have access to key information that is typically reserved for the combat operations center. It provides an avenue for fulfilling John Boyd's belief that "technology and concepts should empower the person, not the other way around."[5] In this case, implementing data-centricity enables Marines to make decisions in a distributed environment when friction and uncertainty abound.

Collectively known as VAULTIS, a data-centric approach makes data visible, accessible, understandable, linked, trustworthy, interoperable, and secure. Data needs to be exposed to a secure environment, so it is *visible* to authorized users. Those users must be able to *access* the data to leverage it. Users must be able to *understand* what the data means in terms of its content, context, and applicability to a given problem set. Data must be *linked* using data formats and metadata tagging to uncover relationships. The data must be *trustworthy* by coming from an authoritative data source so that one can be confident in the data and insights derived from it. Data must be *interoperable* to maintain the semantic and syntactic meaning of the data; otherwise, one risks spurious conclusions. Finally, the data must be *secure* and free from unauthorized use or manipulation.[6]

This is an evolution from the current framework, where data is tied to applications, and the application's capabilities limit the secure utilization of the data. This limits the ability of Marines to utilize the data because exposing the data to advanced analytics and merging it with other relevant data becomes a tedious process of exporting, rationalizing, and importing data. From an operational perspective, it limits the ability of commanders to see inputs from multiple systems in a single integrated common operational picture. In both cases, the architectural framework limits the utility of data and hinders the development of advanced algorithms to include artificial intelligence and machine learning because of the limited amount of data and computing power available.

A data-centric approach can provide an information advantage by reducing the time required to arrive at well-informed decisions, thus increasing the tempo of one's OODA loop. According to *MCDP 1*, "Time is a critical factor in effective decisionmaking–often the most important factor. A key part of effective decisionmaking is realizing how much decision time is available and making the most of that time. Whoever can make and implement decisions consistently faster gains a tremendous, often decisive advantage."[7] Our systems can help make decisions faster by leveraging the right data and applying the right context to it to accelerate the decision-making process. In terms of OODA loops, these systems work within the observation process so that when a commander observes information, it is presented and formatted to speed the orientation process and convey a more accurate mental model for a decision.

Facilitating decision making at the lowest level is imperative given the emerging character of warfare that necessitates decentralized operations. Customized common operational pictures should not only be available at the command post but to the Marines executing the mission as well. The decentralized nature of Marine Corps operations necessitates that Marines have access to as much information as is helpful and formatted in a manner that aids in mission execution.

Implementing Data-Centricity

For the Marine Corps to realize the benefits related to data-centricity, it must innovate within existing paradigms. One of Williamson Murray's conclusions in *Military Innovation During the Interwar Period* was that the most important innovations impacted the context or character of the conflict. Within that volume, Alan Beyerchen proposed three key changes typically occurring for successful innovation. First, new equipment, systems, or devices initiate a technical change. Second is an operational change that refers to how the technical change can be utilized and integrated into other standard operating procedures. Finally, technological change is the resultant "context emerging from the interaction of technical and operational change with each other and the environment."[8] As this relates to data-centricity, the capabilities must

harmonize with Marine Corps operations to out-maneuver an adversary.

Given that data-centricity is an architectural approach and not a solution in and of itself, the technical changes required span a wide array of efforts. Make no mistake, while some of these efforts sound simple, budgetary constraints, dependencies, technical complexity, and myriad other challenges abound. The following list is just an example of *some* of the *high-level* tasks that can improve data-centricity. Ensuring the visibility of data means hosting data sources (cloud, on-premises, tactical edge) so they can be exposed to platforms such as Jupiter, Advana, and Bolt or integrated into applications like Tactical Assault Kit. Perhaps the greatest issue of assuring data access is ensuring resilient, high-bandwidth network transport whether that be provided by satellite communications, fiber optic cables, or other terrestrial means. While this can be challenging for the Marine Corps to execute, this is further complicated when one attempts to extend visibility and access at the joint and coalition levels. This is the heart of Combined Joint All-Domain Command and Control.

Establishing data catalogs, data formatting, and tagging standards are critical for understanding and linking data while ensuring interoperability. This sounds simple, but at the technical level, this can become complicated. Application programming interfaces can enable data to be shared between disparate systems; however, certain systems may need to be modernized to meet certain constraints of that system. To realize the benefits at the tactical edge, programs of record need to modernize not only to share data within an established framework but also so they can evolve as needed based on interoperability with the joint and combined force. Additionally, the data from those systems should be accessible and customizable on handheld devices powered by software such as ATAK.

One element of the operational change refers to how the capabilities can be utilized. At a high level, this means improving how we operate based on the ability to leverage data. For example, could predictive logistics algorithms create a heavier logistics push construct to make the most efficient use of surface and air transport? Could advances in the Manpower Information Technology Systems Modernization drive changes in manpower policy and the way in which boards, assignments, and retention are conducted? Any of these can prove true, but as a Service, we must be willing to evolve the way we operate based on the technical capabilities available.

Another element of operational change relates to how Marines interact with systems to generate data. Marines need to understand that the inputs they make into a given system can have downstream impacts on decision making. For example, if an aviation maintenance department wanted to discover ways to improve readiness by gaining maintenance efficiencies, they could compare data in NALCOMIS OOMA with other relevant data from M-SHARP and other databases. However, if Marines do not log their maintenance time appropriately on a maintenance action form (MAF), it will lead to false conclusions regarding the time to complete MAF. If pilots do not accurately log their flight time or generate MAFs, the resulting data may not reflect reality. In other words, if data is of poor quality, it will either be discarded from analysis which reduces the data points, or it will lead to spurious conclusions. Simply put, if one inputs garbage, the result will be garbage.

The synergy between the technical changes and operational changes can create technological changes that sometimes asymmetrically change the context of our operations. Access to relevant information, formatted in a mission-specific manner when provided to distributed forces, could introduce a new level of maneuver and agility to outpace a more rigid adversary.

Conclusion

History demonstrates that institutions that had an appropriate grasp on the concept of future warfare and were able to balance a better fit between technologies, concepts, doctrine, and organizational change ultimately succeeded over adversaries who failed to do so.[9] The benefits of data-centricity align with the roots of maneuver warfare by enabling Marines to generate speed and tempo by decreasing the time to execute OODA loops. Achieving this benefit requires significant investment in an array of technical and operational changes. Some of these changes can be made at the Service level, but many more require Marines at each echelon to innovate within their command to utilize these capabilities. Implementing data-centricity should not be seen as a buzzword but rather a means to implement elements of *Warfighting* and prepare ourselves as a Service for the next conflict—wherever that may find us engaged in competition, crisis, or conflict.

Notes

1. Headquarters Marine Corps, *MCDP 8, Information*, (Washington, DC: 2022).

2. Wayne P. Hughes and Robert Girrier, *Fleet Tactics and Naval Operations* (Annapolis: Naval Institute Press, 2018).

3. Adapted from John Boyd, *A Discourse on Winning and Losing*, ed. Grant T. Hammond (Maxwell AFB: Air University Press, 2018).

4. Office of the Director of National Intelligence, "The Intelligence Community Data Management Lexicon," *DNI.gov*, January 5, 2022, https://www.dni.gov/files/ODNI/documents/IC_Data_Management_Lexicon.pdf. It should be noted that the use of this definition was directed by the DOD Chief Digital and Artificial Intelligence Officer in a memorandum dated 1 September 2023.

5. Ian Brown, *A New Conception of War: John Boyd, the U.S. Marines, and Maneuver Warfare* (Quantico: Marine Corps University Press, 2018).

6. Department of Defense, *DOD Data Strategy*, (Washington, DC: 2020).

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

8. Williamson Murray and Alan Millett, eds., *Military Innovation in the Interwar Period* (Cambridge: Cambridge University Press, 1998).

9. Ibid.

NOT HOW YOU WOULD'VE DONE IT

YOU BUNDLE THINGS RIGHT

Like when you bundle your home and auto insurance with USAA and save up to 10%.[1]

Visit usaa.com/bundleright to learn more.

USAA®

[1]Savings are off total premium. Not available in all states or in all situations. To qualify for a discount on the property policy, a USAA Auto Insurance policy must be active within 60 days of issuing the property policy. Discount subject to change. Restrictions apply.

Membership eligibility and product restrictions apply and are subject to change.

Property and casualty insurance underwritten by United Services Automobile Association (USAA), USAA Casualty Insurance Company, USAA General Indemnity Company, Garrison Property and Casualty Insurance Company, NOBLR Reciprocal Exchange, based in San Antonio, Texas; USAA Limited (UK) and USAA S.A. (Europe) and is available only to persons eligible for property and casualty group membership. Each company has sole financial responsibility for its own products. Coverages subject to the terms and conditions of the policy.

Accelerating Cyberspace Talent Development and Readiness

People are greater than technology

by Mr. Alfredo Rodríguez III

>Mr. Rodriguez is the current Marine Corps Information Technology and Cybersecurity Community of Interest Manager. He is the Senior Advisor to the Marine Corps Deputy Commandant for Information Workforce Senior Executive and the Deputy C4/CIO Director, Mr. Rodriguez is a former Army Lieutenant Colonel. His experience ranges from battalion command to service on multiple echelons across the Army, including staff and leadership positions in joint and special operations organizations.

The underlying context of the forthcoming Deputy Commandant for Information (DC I) Fighting Smart vision and strategy centers around 21st-century competition and its complexity driven by rapidly changing technology. This requires Marines and civilian Marines to be skilled at exploiting the means of information and technology to out-think, out-compete, and outfight adversaries on every point of the competition continuum in all domains. This goes beyond the acquisition and deployment of decisive and highly deployable technology, extending to an unwavering dedication to total force talent development. If our Marines and civilian Marines do not possess the skills to deploy data, software, algorithms, sensors, and mission-critical technologies effectively, we drastically slow our decision cycle against determined and capable adversaries. To that end, the DC I Fighting Smart vision will lay out a critical pillar to ensure we preserve our most significant asymmetric advantage—people. The Fighting Smart strategy will clearly delineate that people, not technology, are the most crucial resource. A winning future requires a data-literate and technologically adept workforce to achieve systems overmatch.

DC I's commitment to mobilizing talent through a dedicated line of effort underscores this requirement. To that end, the DC I will lead the establishment of a holistic cyberspace workforce qualification program to ensure that our workforce drives enhanced readiness with skilled personnel to win in an ever-changing information environment. A qualified and ready cyberspace workforce is foundational to plan and execute operations that create and exploit information advantages. This line of effort, originally born out of enhanced qualification standards mandated by *DOD 8140*, has now expanded in scope and depth. We are addressing a broader spectrum of work roles no longer limited to legacy cyber and IT functions: artificial intelligence (AI), data science, software developers, and other information-related disciplines will all be encompassed through mobilizing talent. In addition, several resources initially made available to civilians are now scaled to include all Marines and civilian Marines operating in the information environment.

DC I will lead ... a holistic cyberspace workforce qualification program ...

So, what are we doing to mobilize talent?

- Expanding the Defense Cyberspace Workforce Framework (DCWF) implementation to include additional Information work roles.
- Enhancing the offerings for learning and development through our Information Development Institute (IDI) portal.
- Tying our talent initiatives back to readiness through quantitative metrics and data modeling that provide leadership with a better understanding of their individuals' proficiencies and overall workforce capabilities.

Defense Cyberspace Workforce Framework

The DC I team is forging ahead in its implementation of the DCWF, which provides guidance for identifying and tracking the cyberspace workforce (CWF) and lays out the foundation for baseline qualifications, mission support, and continuing developmental

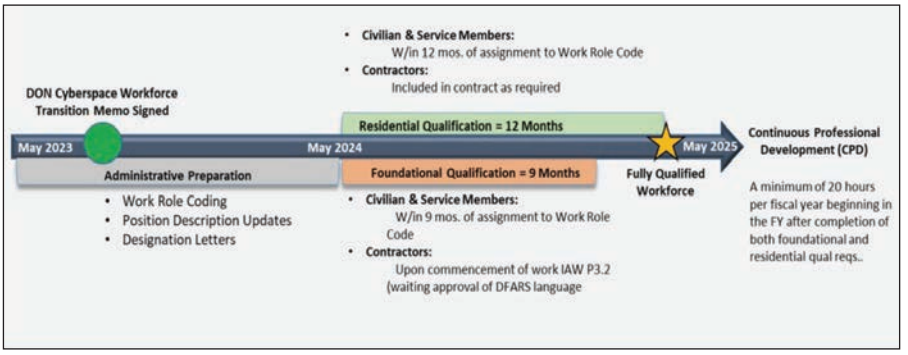


Figure 1. Marine Corps DCWF Implementation (adapted by author).

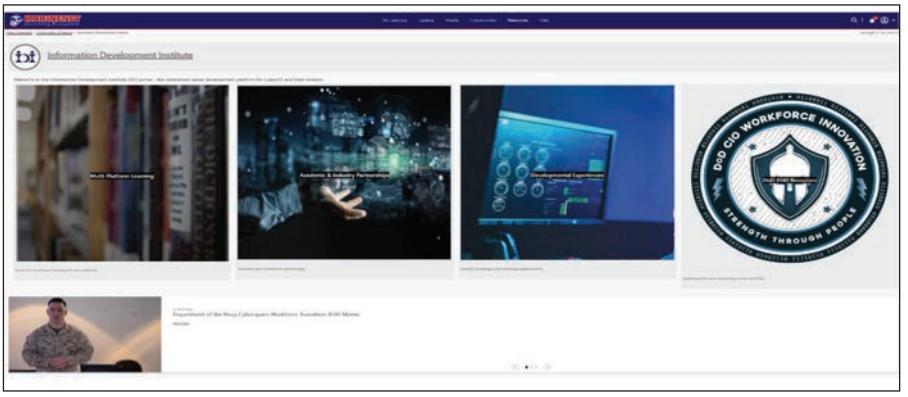


Figure 2. IDI portal featured at MarineNet.[1] ***(Figure provided by author.)***

opportunities. The current *DOD 8140* publications and recent *SECNAV 5239* instructions address the full scope of the CWF. The CWF comprises personnel who build, secure, operate, defend, and protect DOD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; deploy data, artificial intelligence, and software; and project power in or through cyberspace. The deployment of the DCWF includes a standardized way to describe cyber work with the intent of getting the right people in the right positions; we will do this through two main efforts: cyber work role coding and qualification.

Marine Corps implementation of DCWF follows a two-year phased approach. Year 1 activities, currently in progress, ensure all positions performing cyberspace activities and support are coded correctly. This "coding" activity includes designating billets and positions within the DCWF through the implementation of three-digit codes in respective manpower data systems. Additionally, Year 1 activities include civilian position description updates, DCWF designation letters, and ensuring our human capital (manpower and personnel) data systems are prepared to support the implementation of the DCWF.

Starting in May 2024, DC I Information Workforce team will shift to Year 2 activities that focus on preparing Marines and civilian Marines to qualify for the work role they are performing. DCWF personnel must foundationally qualify using identified MOS or occupational series-specific training, education, or certification. A composite qualification reference is pending publication this spring from the DOD chief information officer. Additionally, the CWF must demonstrate residential qualification, which builds upon foundational knowledge, bringing personnel up to speed and expanding their skills through a training and development program. On-the-job development and training programs are vital for developing newly recruited or hired workforce personnel and upskilling and retaining talent. Residential

qualification is a combination of on-the-job training that supports familiarization with a position, system, or seat, followed by environmental-specific requirements derived from position and organizational mission requirements. All of this gets wrapped up as part of a developmental plan and enhanced with continuous professional development across the individual's Marine Corps career.

Information Development Institute:

In 2021, the IDI was piloted to provide quality training, education, and experiences to improve IT, cyber, and data/AI workforce skills and competencies for civilian Marines who had no established training continuum. During the evaluation of this pilot, the DC I workforce team found that IDI could not only be successful at providing opportunities to civilian Marines in the cyber workforce but also across the entire Marine Corps CWF, including active and reserve Marines: a total-force solution. DC I team plans to codify this expansion in a forthcoming MARADMIN.

The IDI resides on the MarineNet eLearning ecosystem and offers quality training, education, and experiences to improve IT, cyber, and data/AI workforce skills and competencies. The IDI provides an opportunity for continuous development for cyber Marines and civilian Marines to explore three major avenues of training: multi-platform learning, academic and industry partnerships, and developmental experiences. Those focus points are dictated by using the DCWF as a foundation to provide access to in-person or online learning resources, awareness of educational opportunities, and insight into rotational experiences. The IDI includes vendor learning platform subscriptions and Marine Credentialing Opportunities Online program access. The Credentialing Opportunities Online program helps cyber civilians and officers find information on paying for costs associated with initial credential attainment and maintaining and renewing those credentials. The IDI also features offerings from the Marine Corps Cyber Auxiliary (MCCA). The MCCA utilizes volunteer subject-matter experts from cyber communities outside the DOD and asks them to give free courses to the Marine Corps. The MCCA has gathered over 400 volunteers from numerous subjects across cybersecurity, and all of them are ready and willing to volunteer their time to help educate the Marine Corps on the topics they are most proficient in. Lastly, the DC I team is working with the DOD Chief Data and AI Office to expand its data/AI offerings. This will include additional data/AI training opportunities through partners and industry vendors, providing courses for Azure cloud AI and zero-trust architecture, and launching courses to foster software development and engineering.

The IDI resides on the MarineNet eLearning ecosystem ...

Visualizing CWF Readiness Through Workforce Analytics

With the official qualification timeline for DCWF kicking off in May 2024, the DC I team has begun to lay the foundation for how DCWF data will be aggregated to determine compliance, provide useful reporting to leadership, and drive workforce readiness. The framework of distinct workforce categories, work roles, and proficiency levels enables detailed and granular visualizations of workforce and qualification gaps that can be addressed with targeted recruitment and development efforts.

The DC I Information Workforce team initiated the process of visualizing CWF qualifications, identifying data sources, establishing processes, and building visualizations. This centers on a partnership with existing data capabilities, including the Bolt warfighting data cluster within the Department of the Navy's Jupiter data analytics environment, to provide a centralized platform for consolidating human capital data securely and responsibly. Through our workforce analytics initiative, the DC I team is developing and publishing visualizations (i.e., data-driven dashboards) to accomplish these primary objectives:

- Maintain current and comprehensive workforce metrics.
- Report on 8140 compliance.
- Establish workforce proficiency baseline and trends.
- Provide workforce inputs to overall information readiness.

Workforce data is a key strategic asset to provide clarity on demand and actionable insights to assist leaders in shaping the readiness of the information workforce.

Conclusion

The first line of effort in the DC I's Fighting Smart Campaign plan centers on developing, retaining, and employing skilled Information-Age personnel. The intent is to mobilize talent to adapt and innovate in the new realities of cyberspace and the information environment or find ourselves reacting to more attentive and agile adversaries. The cognitive fight will be the deciding factor in who prevails. The DC I team accelerates talent development in this domain by recognizing and fully embracing cyberspace and information as a core competency. Implementing the DCWF, in alignment with the DOD and Department of the Navy cyber workforce strategies, helps the Marine Corps assess and develop this critical workforce, improve retention efforts, and foster skill advancement across all proficiencies and experience levels. Data analytics of the CWF will drive improvements in workforce planning, human resource support, and talent development initiatives. A data-driven, agile, and cyber-ready workforce is the key asymmetric advantage to succeeding in this transformational warfighting domain.

Notes

1. Staff, "Information Development Institute," *MarineNet*, n.d., https://portal.marinenet.usmc.mil/IDI.html.

PLEASE VISIT OUR BOOTHS AT THE MODERN DAY MARINE EXPO.
WE LOOK FORWARD TO SEEING YOU THERE!

USAA® BOOTH 2343 | BAE SYSTEMS BOOTH 1614 | ManTech. Securing the Future BOOTH 2933

AIRBUS U.S. SPACE & DEFENSE BOOTH 2415 | ALTAEROS BOOTH 333 | ASTRONICS TEST SYSTEMS BOOTH 1343 | RHEINMETALL BOOTH 1033

BLUESKY INNOVATIONS BOOTH 2217 | CUBIC Defense BOOTH 2143 | ECHODYNE BOOTH 1215 | ESS BOOTH 1643

FLYER DEFENSE BOOTH 2607 | FOCUS MARINES FOUNDATION WHERE THINGS START TO GET BETTER BOOTH 3047 | GENERAL DYNAMICS BOOTH 1606

GENERAL ATOMICS AERONAUTICAL BOOTH 1407 | leidos BOOTH 1321 | LEONARDO DRS BOOTH 2521

LGL BOOTH 2454 | MANTIS BOOTH 456 | NORTHROP GRUMMAN BOOTH 1433 | OneWeb Technologies BOOTH 154

OSHKOSH DEFENSE BOOTH 1915 | PACIFIC DEFENSE BOOTH 2925 | Parker BOOTH 2542 | PARSONS BOOTH 3114

PERSISTENT SYSTEMS BOOTH 937 | POLARIS BOOTH 1633 | Skydio BOOTH 2851 | SMARTSHOOTER BOOTH 533

tagup BOOTH 517 | TELEDYNE FLIR Everywhereyoulook BOOTH 1333 | TRANSHIELD BOOTH 2442 | Veterans United Home Loans BOOTH 910

MODERN DAY MARINE

THE MARINE CORPS ASSOCIATION IS A PROUD CO-HOST OF MODERN DAY MARINE

MARINE CORPS ASSOCIATION

The Key Enabler to Force Design is Over-the-Air Connectivity

Access to space will determine the force's ability to persist, sense, shoot, and ultimately prevail in a future fight

by CWO4 Emedin Rivera

The Marine Corps's value proposition to the Joint Force is its ability to organically sense, persist, maneuver, and shoot inside an adversary weapons engagement zone (WEZ) in support of a broader naval campaign. To achieve these core objectives evolved MAGTF formations must consider connectivity a central precondition to the success of the force. Expeditionary advanced base operations (EABO) is a principal concept in the force's ability to operate inside actively contested maritime spaces:

> Definition. EABO is a form of expeditionary warfare that involves the employment of mobile, low-signature, persistent, and relatively easy-to-maintain and sustain naval expeditionary forces from a series of austere, temporary locations ashore or inshore within a contested or potentially contested maritime area to conduct sea denial, support sea control, or enable fleet sustainment.[1]

There is clear and compelling evidence across academia, inputs from the fleet, and real-world conflicts in Europe that space-enabled data transport is one of the most indispensable resources maneuver forces need to compete in today's battlefield. Beyond line of sight (BLOS) over-the-air (OTA) connectivity is central to Force Design, EABO, and the success of future campaigns. Implicit in the effective execution of EABO is the ability to connect large quantities of integrated sensors, long-range precision shooters, and mesh sustainment networks to command nodes thousands of miles apart. This problem can only be solved by one key enabler: OTA connectivity.

>CWO4 Rivera is the Space & Waveform Integration Officer, Headquarters Marine Corps, IC4.

Fundamental to achieving information overmatch is achieving disaggregated OTA connectivity to every node in the network to include the most disadvantaged. Target, location, sustainment, and other essential data necessary to gain and preserve an advantage against an adversary are marginally useful without quality connectivity. Lower echelons of command and novel formations like Marine littoral regiments demand exponential growth in broadband connectivity to support long-range sense and strike, cloud replication, unmanned system control, principles of zero trust, and much more. Data and endpoints are but a small part of a broader information ecosystem in which connectivity underwrites mission success or failure.

... space-enabled data transport is one of the most indispensable resources ...

Hyperconnectivity, a Precondition for Effective EABO

In today's fight where speed, dispersion, and standoff distance between both friendly and adversary forces are held at a premium, BLOS OTA connectivity is an indispensable resource that yields outsize competitive advantages to commanders across all echelons of command. The curvature of the earth artificially concentrates maneuver forces in line of sight (LOS) communication kill boxes and prevents forces from massing from a disaggregated and dispersed position of advantage. Direct-to-node data delivery and massing without concentrating can only be enabled by assured, abundant, layered, high-quality BLOS OTA connectivity.

> The littoral force's firing units must be capable of receiving firing data from multiple sources: forward observers, reconnaissance assets, aircraft, adjacent units, tactical headquarters, or even directly from the maritime operations center (MOC). Regardless of the source, firing units receive targeting data directly rather than through several echelons of the task organization.[2]

Line-of-sight systems hold maneuver forces at risk because they come with reduced mobility, increased force pro-

tection, and logistical overhead. The demands to support these nodes make them prohibitively costly. Overhead aerial relays and battlefield airborne communications nodes do not fare much better than terrestrial static relay sites in a future fight. Against mature anti-access/area-denial complexes, battlefield airborne communications nodes become priority targets and are inevitability forced outside the adversary's WEZ rendering them ineffective. Hence, terrestrial retransmission and aerial relay nodes should only be considered additive to core architectures that do not depend on static platforms to operate. The next fight is an on-the-move BLOS fight, and it almost exclusively depends on access to space.

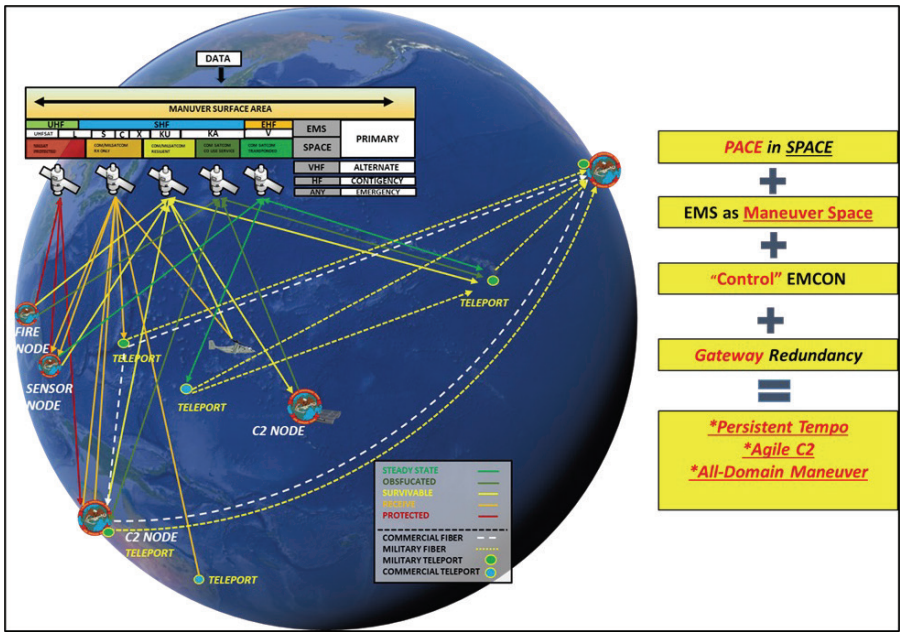


Figure 1. Dynamic PACE.

No Space, No CHANCE!

The Deputy Commandant for Information, LtGen Glavy, often speaks about the indispensability of space. He coined the phrase, "*No space, no chance.*"[3] The force's clear dependency on space may invoke a strong desire to wire in the defense or break out the old field phone and double down on disconnected, denied, intermittent, limited (DDIL) bandwidth techniques that require running yellow canary messages to the watch officer. Disconnected, denied, intermittent, and limited is a false choice whether self-imposed or not. The force cannot afford to be disconnected. To be disconnected is not a mild inconvenience or a passive cost of doing business; rather, it is a paralyzing condition that denies maneuver forces its core mission objectives.

> To accomplish their tasks, infantry battalions must be organically equipped, starting at the squad level, with resilient, networked communications and precision fire capabilities, including loitering munitions enabled by artificial intelligence. These units must be light, mobile, and capable of distributed operations.[4]

To be disconnected is unacceptable and must actively be combated with the deployment of timely abundant, layered, broadband connectivity and the full arsenal of a communicator's skill. Exponential availability of broadband connectivity at the tactical edge is particularly important in the areas of edge cloud computing and artificial intelligence (AI).

> Constraints arise based on the application or model onboard the device. For example, large language models are a particularly computationally demanding type of AI and can be impossible to run on some devices. One such model, OPT-175B, is partitioned across 16 high-performance Graphics Processing Units (GPUs)-far more compute than is available on the edge devices explored in this report.[5]

The inference is that replication to AI and high-end computing tools require abundant, layered, broadband connectivity based on inherent onboard AI constraints and limitations.

Fieldcraft, awareness of geography, power management, emission control comparable to the threat, and stacked primary communication plans also require retooling. Primary, alternate, contingency, and emergency (PACE) plans are key to actively combating DDIL. Most PACE plans are linear and anchor on single-path transport media. They neatly move down a predictable scale where bandwidth is the limiting factor and battle staffs must drastically change processes to cope with disruption. However, conditioning commanders with linear PACE plans sets conditions for artificial disruptions in tempo and real losses on the battlefield. A dynamic PACE plan preserves tempo by prioritizing data for combat advantage (video, voice, text, file transfer, variable message format) and treats transport holistically as maneuver space. A dynamic PACE plan maneuvers across waveforms, bands, and orbits without disrupting tempo. A linear PACE plan is passive while a dynamic PACE plan actively seeks combat advantage by proactively maneuvering based on evolving intelligence and environmental factors.

Dynamic PACE

Unfortunately, a combination of culture, understanding, and messaging presents a collective threat that seems unsurmountable. This is especially true if you consult intelligence reports without context or depth. There is no doubt Marine Corps connectivity is held at risk by credible capabilities. However, we should be precise in our messaging and at all costs avoid creating a culture of fear and self-denial. "Space is the most resilient capability we have," LtGen Glavy said according to *Defense News*, "I'm telling you right now: We don't win the space domain? Don't bother."[6] The collective toolbox for countering these credible threats is expansive, diverse, and only getting

better. However, it requires a reimagining of how we think about space-enabled data transport. Space-enabled data transport is not a program office or a bespoke waveform, orbit, network, band, or other key technology. It is a diverse but unified ecosystem of transport options that can be terminated and federated at key sites across the globe. It includes the electromagnetic spectrum, commercial and military on-orbit capabilities, optical backbone, gateways, and waveforms. The advancement of optical relays, full terminal mobility, high throughput satellites, software-defined modems, the proliferation of new orbits, industrial iteration speed, and vertically-integrated supply chains make space-enabled data transport an indispensable ecosystem required for achieving asymmetric advantage in great-power conflict and credible deterrence in competition.

Speaking on Ukraine at *Brookings*, Gen Berger said, "The power of information at the local level and the ability to move it almost all of it unclassified, amazing ... to operate at speed you have to look at some unconventional ways to move information."[7] The components of the space-enabled data transport ecosystem, whether dual-use spectrum, waveforms, protected military bands, or commercial infrastructure are all maneuver space and combined, provide a system that serves to assure the forces' ability to sense, persist, maneuver, and shoot across the range of competition to conflict. The dilemma for the adversary is not in any single key technology; it is in the diversity of options that may be available to the Marine on the ground at any given time. Diversification of the transport environment inherently imposes costs on the cognitive and technical capacity of even the most capable adversaries.

The full range of space capabilities is necessary to mass capacity and exhaust an adversary. The Service must not create artificial scarcity by policy or procedure and instead position the force to take maximum advantage of the exponential growth in commercial space. Commercial space is uniquely positioned to bring the Corps concepts of highly disaggregated and distributed forces into relevant, credible, and effective capabilities. Formations like littoral combat teams (LCT) and littoral anti-air battalion demand assured connectivity beyond existing authorized acquisition objectives (AAO) to effectively disseminate target data and other critical information. "Littoral Combat Team (LCT) based on an infantry battalion but also possessing an anti-ship missile battery, a Littoral Anti-Air Battalion, and a Combat Logistics Battalion. The LCT will focus on the employment of platoons, which is radically different from a standard battalion's use of companies."[8] The viability of LCT deployments is heavily contingent on rapid exchanges of data across vast distances enabled by abundant, layered, broadband OTA connectivity. As experimentation and iteration reveal OTA connectivity as a foundational precondition to force development success, the Service must stand ready to rapidly integrate commercial space capabilities swiftly.

Ukraine, Harbinger of Change

The preliminary lessons of Ukraine almost prophetically reinforce the operational assumptions of Force Design and EABO. These lessons highlight the outsized impact of space-enabled data transport on the battlefield. The Armed Forces of Ukraine (AFU) created in short order an environment of opportunistic connectivity where all options were welcomed. They accepted risk in their architecture and combined speed, fieldcraft, and maneuver to maintain the advantage. They used unencrypted communication paths to flood the zone and significantly improved their information maneuver surface area by using commercial off-the-shelf options to impose technical and cognitive costs on the adversary. "First, Ukraine has developed truly connected, high-speed command and control."[9] Their novel surveillance and strike techniques were only possible by their "connected, high-speed command and control." AFU accepted risk and disrupted the paradigm of inevitable Russian dominance by integrating new capabilities at speed.

Ukraine's networked drone programs allowed remote pilots to feed realtime targeting data across vast distances back to High Mobility Artillery Rocket System launchers out of adversary range. This enabled very precise strikes on ammunition depots, bridges, and staging areas essential to

Table 4.2. Emerging Commercial Satellite Communications Technologies That the U.S. Department of Defense Can Leverage

Technology Type	Description
Rapid ad-hoc networking	Temporary networks that enable communication between terminals without routers or other intermediaries
Transponder lease with protected tactical waveform (PTW)	Leased commercial transponders hardened with PTW
Small spot beams	Higher power signal concentrated in a specific region
Steerable beams	The ability of a satellite to control where it is providing coverage within a specific region
Beam forming and nulling	Signal filtering outside a desired spatial region that increases jamming resistance
Intersatellite links	Communication between satellites that increases resilience
Software-defined radios	Adaptive and reconfigurable systems enabled by software
High- and very high-throughput satellites	Satellites that can support significantly higher throughput capacity without requiring additional spectrum access
Frequency diversity	Greater diversity of frequencies utilizied
Adpative link power and bandwidth control	Bandwidth optimization that improves resource use efficiency

Leveraging emerging commercial satellite communications technologies. *(Source: Rand Corp., Wong (2022).)*

Russian assault preparations. Local militia forces using commercial satellite phones and messaging apps were able to instantly relay convoy sightings and troop movements to territorial defense battalions dozens or hundreds of miles away, enabling rapid ambushes. Intercepted Russian communications were even crowd-sourced across civilian networks to help target battlefield commanders.

The common use of commercial off-the-shelf terminals, commercial drones, and unmodified consumer tech allowed ad-hoc infantry networks to fuse open-source intelligence feeds from across the country into a realtime targeting and threat tactical picture much more responsive than many legacy command systems today. AFU employed approaches to comms that most consider "worst practices" to great effect. Seems clear that overly emphasizing encryption, certifications, and cybersecurity leads to vulnerability of tempo and opportunity. The Marine Corps must not fortify with the expectation of safety but instead build resilience with the expectation of attack. Agility and reconstitution demand more options not less and should not be restricted by artificial limits centered on incentives of risk aversion.

Adapt and Win

As previously mentioned, commercial space capabilities deliver outsized combat advantage and directly contribute to our commander's ability to achieve information overmatch in the next fight. The Marine Corps must rapidly integrate and deliver these capabilities while keeping pace with industry. Today, the Service largely operates outdated terminals that are not able to consume advanced commercial space capabilities. Although the focus tends to be on terminals, the real operational value is not with the endpoint/terminal. The value is on the space services the terminal can consume. Our fielding of dated terminals must shift to mission-focused service consumption of advanced commercial space capabilities. No one worries much about Dell versus HP laptops today. Rather, what services or resources can I access and consume?

Risk reduction can be achieved with commoditized modularity versus standardized, one-size-fits-all combo terminals that are tied to archaic tri-band requirements. A single-terminal approach—although popular—is not optimal. It creates single points of hardware failure and makes terminal maintenance much more costly to the unit. It also makes the supply chain vulnerable to single-component disruption. Commoditized dual terminal solutions optimized for advanced commercial space services would create a much more resilient approach. "Leveraging services from multiple commercial service providers that use dissimilar or heterogeneous technologies (and have dissimilar

vulnerabilities) adds resiliency, which in turn mitigates many of these risks, as can adoption of new tactics, techniques, and procedures."[10]

The Corps must adopt a more agile approach to delivering connectivity to the force to reduce risk in future force development as it matures in stride. Legacy acquisitions assume the program objective memorandum process adequately projects capability needs to meet the demands of an actively evolving force. However, there is a growing consensus it does not deliver the necessary agility to compete. Iteration speed is a key marker of competitive advantage. Opening the aperture to multiple commercial space service providers in a novel more agile approach will deliver combat advantage across all echelons of command. Focusing on the commercial service and not the endpoint will allow access to a global, non-military attributable gateway architecture and will deliver pure commercial spectrum, waveform, gateway, orbit, and spacecraft options which will inevitably complicate the adversaries targeting cycle.

To this end, the Corps is leading in creative new approaches informed by FMFs and organizations like the RAND Corporation to make meaningful strides forward.

> Gaining operationally useful capabilities from commercial space services will require ... remove barriers that limit commercial services from being fully integrated into military operations ... Increase the sophistication of contracting capabilities to be more adept at negotiating contracted services. Build flexible resourcing options so that service contract negotiations can be conducted in a more timely fashion.[11]

The Corps is delivering adaptable and disruptive connectivity options to the force today via creative contract line-item numbers structures that provide a release pressure valve for the fleet to surge, pivot, or reconstitute capability at speed. This novel approach relieves the lag in programmatic systems compared to the pace of technological change. It establishes well-resourced service models that generate material solutions under service contracts in a much more adaptable and responsive way to the demands of the force. It alleviates the sunk cost of ownership and the burden of lifecycle sustainment from research and development to disposition. It reduces risk to rigid ten-year cycles where adaptability is not a virtue. It augments our legacy inventories with hybrid service/lease models that employ dual-use technology and fully leverage independent research and development of industry, speed, and production throughput of dual-use systems.

The Corps must adopt a more agile approach to delivering connectivity to the force to reduce risk in future force development as it matures in stride.

Conclusion

The commercial space industry is accelerating into unprecedented new frontiers, launching new satellites and transport layer capabilities at an exponential pace once unimaginable. This flood of emerging technologies and potential partners presents both immense opportunity and potential peril for Marines. Maintaining a decisive asymmetric edge and connecting Marines to the power of information at the point of need in a future fight requires our methods to drastically transform. Failure to keep pace with commercial space innovation risks creating near-peer parity, or worse, a capability deficit in coming years instead of decades. Systems fielded a decade too late will continue to levy considerable logistical burden on units without the benefit of capability that delivers real combat advantage. For these reasons, the Marine Corps is setting conditions to bring novel adaptable methods to enable access to assured, abundant, layered, BLOS OTA connectivity to the force today.

Notes

1. Headquarters Marine Corps, *Tentative Manual for Expeditionary Advanced Base Operations*, (Washington, DC: 2021).

2. Ibid.

3. C. Demarest, "U.S. Must Dominate in Space to Win Future Wars, Marine Corps' Glavy Says," *C4ISRNET*, December 11, 2023, https://www.defensenews.com/battlefield-tech/space/2023/12/11/us-must-dominate-in-space-to-win-future-wars-marine-corps-glavy-says.

4. *Tentative Manual for Expeditionary Advanced Base Operations.*

5. A.J. Lohn, "Onboard AI: Constraints and Limitations," *CSET,* August 2023, https://cset.georgetown.edu/publication/onboard-ai-constraint-and-limitations.

6. "U.S. Must Dominate in Space to Win Future Wars, Marine Corps' Glavy Says."

7. Brookings Institute, "21st Century Soldiers of the Sea: A Convo with General David Berger the U.S. Marine Corps," *YouTube* video, 1:10:25, May 23, 2023, https://www.brookings.edu/events/21st-century-soldiers-of-the-sea-a-conversation-with-general-david-berger-38th-commandant-of-the-us-marine-corps.

8. D.L. Wood, "Executive Summary of the 2023 index of U.S. Military Strength," *The Heritage Foundation*, October 2022, https://www.heritage.org/military-strength/executive-summary.

9. T. Hammes, "Game-changers: Implications of the Russo-Ukraine War for the Future of Ground Warfare," *The Atlantic Council*, April 2023, https://www.atlanticcouncil.org/event/game-changers-or-little-change.

10. J.P. Wong, "Leveraging Commercial Space Services," *Rand Corp*, September 2022, https://www.rand.org/pubs/research_reports/RRA1724-1.html.

11. Ibid.

DELIVERING ENTERPRISE-WIDE CAPABILITIES FOR TOMORROW'S MARINE CORPS, TODAY

U.S. Marine Corps photo by
Lance Cpl. Matthew Morales

leidos

Cyber in Support of the Marine Littoral Regiment

Assuring C2

by Maj Aric Anthony

>Maj Anthony is the 3rd Marine Littoral Regiment's Cyber Planner. Previously, he served at Fort Meade working with the National Mission Team. Before attending the Cyber Center of Excellence, he was the Task Analyst for the 17XX and 06XX Occupational Fields. Prior to becoming a Cyberspace Officer, he was a Communications Officer.

Cyber Marines integrated at the regimental level now play a critical role in enabling warfighting. As the Marine Corps continues to implement *Force Design 2030*, it must continue to experiment and refine its approach to less familiar domains such as cyberspace. Over the past five years, the integration of cyberspace operations within the FMF has proven indispensable and has risen to the challenges of an evolving Service. Cyberspace warfare Marines have aggressively pursued *Force Design 2030* aims and facilitated significant operational outcomes. Successful planning and execution of cyberspace operations requires planners with a keen understanding of the operational environment and authorities as well as the ability to effectively align tactical objectives with Marine Corps and Joint Force operational objectives. The *placement and access* of Marine littoral regiments (MLR) aid the success of cyber operations at the tactical level. To continue to expand in capability to explore what is possible, forthcoming development and experimentation necessitates a strategic emphasis on *assuring command and control* (C2) for FMF operations, thus maturing partner force relationships.

Since establishing the 3rd MLR in 2022, cyberspace operations have contributed to the MLR's advancements and, subsequently, the greater FMF. During Integrated Training Exercises 1-22 and an MLR Service-level Training Exercise 1-23, defensive cyberspace operations (DCO)-internal defensive measure (IDM) Marines were attached to the regiment to monitor and defend an AN/TPS-80 Ground/Air Task-Oriented Radar. The Ground/Air Task-Oriented Radar is a multi-mission air surveillance system that can detect, identify, and track airborne threats common to combat environments. These include cruise missiles, aircraft, and remotely piloted vehicles, as well as rocket, artillery, and mortar fire. Protecting this asset greatly enhances the MLR's ability to conduct air surveillance and air control operations. During MAGTF Warfighting Exercise 2023, the same DCO-IDM formation operated at the MLR headquarters, integrating with regiment communicators and the 3rd Network Battalion to *hunt and harden* the regiment's key terrain in cyberspace. As communicators focused on *enabling* C2 and ensuring network availability for the regiment commander and staff, DCO Marines hunted MLR key terrain in cyberspace for malicious cyber activity and network vulnerabilities to *assure C2*, sharing *realtime* information on anomalies with communicators and network defenders. During Balikatan 2023, a forward-deployed element from U.S. Cyber Command integrated with MLR and helped codify *request-for-support* processes for the new Marine Corps Information Command (MCIC) to enable a tactical Marine formation. In the modern battlefield with a peer adversary, control of this key terrain in cyberspace will prove every bit as helpful or harmful as physical key terrain has shown to be in the past.

Due to their composition and mission, MLRs are uniquely postured to leverage cyber capabilities to enable effects at the tactical and operational levels. As part of the Stand-in Force, the 3rd MLR's mission is *to disrupt the adversary in a contested littoral environment through reconnaissance, counter-reconnaissance, and sea denial operations to support the maritime campaign*. Unlike the cyberspace planners throughout the other MEF formations and Service-component commands (SCC), the MLR cyberspace warfare officer and chief are focused on MLR-specific problem sets and Service-level training events for three years. The MLR's mission also enables cyberspace warfare officer to routinely integrate and train with the partner forces, building and maturing a shared understanding of adversarial threats in cyberspace and each element's defensive cyber capabilities. The MLR's partner force relationships are a key conduit between U.S. Cyber Command, the MCIC, FMF, and regional partners. In contrast, MEF and SCC cyberspace planners are responsible for dozens of exercises across INDOPACOM. These planners do not have the requisite time or staff to manage and further develop in-depth relationships with partner nations while leading up to planning

conferences and post-exercise. The 3rd MLR's cyberspace warfare Marines have the advantage of both the *placement and access* to plan, integrate, and enable cyberspace operations in FMF operations throughout the MLR's assigned area of operations. To this end, commanders, staff, and cyberspace operations planners across the Service must understand how various information warfighting and cyber capabilities support and enable SLTE and stand-in force operations, activities, and investments (OAI) throughout the competition continuum.[1]

Effective communication has always been a lynchpin for successful tasking and execution. This is where the information operations sections within the FMF can improve. One approach is streamlining pathways between the MLR, MEF, and Marine Corps Forces Pacific Command cyberspace warfare Marines through battle rhythm events, OAIs, SLTE, and Joint Level Training Exercise conferences. Until the cyberspace warfare structure and expertise grow, division planners and information warfighting stakeholders must also be included in these same battle rhythm events and touchpoints. Next, cyberspace operations planners require access to requisite repositories and capabilities and leverage the radio battalions in the interim. Finally, effective integration with the MCIC and MARFORCYBER, namely its Marine Corps Cyberspace Group and Marine Corps Cyberspace Warfare Group will aid in a codified cyber operations plan prior to operations. Constant communication and coordination with the groups and their subordinate formations are vital to the effectiveness of 3rd MLR cyberspace operations' support Marine Corps and Joint Force operational objectives in the Indo-Pacific region.

Assured C2 facilitates effective issuing of orders to distributed forces and the coordination of maneuver and fires across the warfighting domains possible. As cyberspace operations at the tactical level mature, a phased approach to DCO is needed to achieve effective cyberspace operations throughout the first island chain. 3rd MLR is uniquely positioned to execute enduring missions with partner forces in the region. To exploit this opportunity, the MLR can leverage the Marine Corps Cyberspace Group and its network battalions' mission to *secure, operate, and defend* the Marine Corps Enterprise Network (MCEN). The MLR commander must know that his key terrain in cyberspace overwatch is established, monitored, and secured before conducting operations. Before, during, and post-operations, MLR's S6 and cyberspace warfare officer coordinate and ensure active network monitoring and defense as well as DCO hunting and hardening missions, respectively. MLR forces must register their warfighting systems, software, and networks that do not operate within the MCEN. Once identified, the systems that tie into the MCEN must be remotely or locally monitored, thus requiring the support of DCO-IDM forces and capabilities. Here is where the importance of cyberspace operations planners' engagement at OAI CDCs and IPCs to determine these requirements. Once the MLR or elements are forward deployed, the MLR cyberspace operations planner transitions *training, advising, assisting,* and *accompanying* partner forces in cyberspace operations to harden their networks and systems. By having our partner networks secure the commander does not have to worry if the scheme of maneuvers or fire support plans are compromised if shared with our partners due to the partner networks being compromised, thereby further enabling the MLR's lethality.

At the tactical edge, cyber planning, resources, and requirements from the MCIC and MARFORCYBER must be nested to ensure they are working with the national cyber protection team or Service cyber protection team. First, this starts with the partner nation asking for national cyber protection team assistance. After an assessment, the remediation plan is given to a Service cyber protection team for follow-up on coordination and advisement. Once the foundation is set, this mission is pushed to the FMF (DCO-IDM) and added to the battle rhythm. The transition is the key after the initial assessment. It is beneficial to have a familiar face working with the partner. Due to the MLR having a specific area of responsibility, their planners should be a part of the initial group presenting the remediation plan. Once the remediation plan starts, the relationship continues throughout exercises, and the periodic check-in will reoccur due to the persistent placement and access the MLR has. The final step is transitioning from a DCO-focused mission to contributing to the overseas contingency operations mission set. This starts with understanding the targeting process and becoming involved via participation and advocating non-kinetic targeting prioritization. This ensures all bases are covered not just from a defensive perspective but also provides insight from the tactical edge on what contributes to survivability and lethality.

Cyberspace operations within the FMF have proved necessary and integral to SLTEs and 3rd MLR's operations since its establishment in 2022. *Force Design 2030* has been implemented with success through the positioning of cyberspace warfare Marines who work closely with the regiment commander and staff to enable unit success as well as follow division-level objectives that support training and wider cyber objectives. By continuing to mature and tighten MLR cyberspace relationships with partner forces, the Marine Corps can generate more effective training exercises, support assured C2, and a more lethal force. Although there has already been an established level of success, the advances made to date serve as a harbinger of the good that can continue to flow back to the Marine Corps when cyberspace planners are properly placed, supported, and understand the operational environment and authorities to align tactical objectives with Marine Corps and Joint Force operational objectives.

Notes

1. Department of Defense, *Department of Defense Cyber Strategy 2024,* (Washington, DC: 2024).

The Military Matrix Structure

Let us make it work

by Maj Lawrance Andrus Jr.

Before discussing any criticisms, defining the military matrix structure (MS) is essential. The military MS, also known as a "matrix structure," is a type of organizational structure that combines multiple lines of authority within one organization. Typically, in an MS, individuals have two reporting relationships: the manager and the product manager. This could mean that a Marine reports to a geographical and functional commander, such as intelligence, operations, or logistics. The purpose of this structure is to merge the strengths of both vertical hierarchies and flat, functional structures. Its objective is to be more flexible, responsive, and adaptable in dynamic environments like those encountered during military operations. Now that we have clarified what the MS entails, we can explore any criticisms or areas of concern. An infantry battalion's headquarters and service company serve as an example of this type of organization.

>Maj Andrus is a Communications Officer. He was deployed to Marjah, Afghanistan, in 2011 with 2/9 Mar, and to Iraq in 2020 with the 2nd Marine Raider Battalion. Currently, he serves as the G-6 Operations Officer at 2d MLG.

The Infantry Battalion as an Example

This structure of organization centers around the commander and his staff. Each staff member leads their respective sections or platoons. For clarity, we identify these sections as "functional departments." Each functional department supports the battalion and any attached agencies and complies with external agency requirements, including immediate higher headquarters. This compliance allows the organization to adapt to policy changes in realtime. We identify the leaders of these functional departments as "functional managers." These managers have two prominent roles. They execute their office's duties under the battalion commanding officer's guidance, leadership, and vision. They also lead and manage the Marines in their department, showcasing the skills and qualities their office demands. The functional aspect represents half of the military MS. The other half pertains to the products the functional departments provide to the supported units. For instance, the S-1 (administrative section) offers administrative support to all primary purposes. The headquarters company, housing all the battalion's functional departments, provides the services. This structure is where MS dominates the organization.

What is MS

The military MS represents a "structure that creates dual lines of authority and combines functional and product departmentalization."[1] This structure groups MOS to foster a monopoly of knowledge and product efficiency. It also enables the unit to employ the economy of force for supported units. For instance, an intelligence officer might assign an intelligence analyst to an infantry company to optimize intelligence products. This assignment enhances information sourcing and gathering because of the detached Marine's vast knowledge and expertise.

The military MS, also known as a "matrix structure," is a type of organizational structure that combines multiple lines of authority within one organization.

produce items mandated by directives, orders, or other standard procedures. These items might include naval correspondence, award administration, and workforce management. The management of these products falls under the product managers: usually, the headquarters company or headquarters section within a headquarters unit. The "straight leg" companies consist of three infantry companies and one weapons company. Generally, these units serve This approach exemplifies the economy of force, as the entire S-2 (intelligence section) dedicates only a portion of its resources to support the infantry company directly with the detached intelligence Marine facilitating this. However, this structure has a notable drawback: it compromises the warfighting principle of unity of command. This issue mainly affects the headquarters company of an infantry battalion. Functional managers report to two superiors. The

battalion commander is their primary superior, focusing on the functional departments, managers, and the products each section produces. The secondary leader, the headquarters company commander, focuses on the Marines' service leadership. While this distinction might suggest no conflict between the two superiors, headquarters company commanders often believe they oversee everything "under their charge." This perception frequently leads to role conflicts within the organization, especially between the functional managers and the headquarters company functions.

Example 1

As a communications officer, I served the S-6 section. When a product in the S-6 section did not meet readiness standards, I collaborated with the S-4 (logistics) section to address the issue before presenting our findings to the battalion executive officer. We did not need direct input from the battalion commanding officer because we acted within his intent and *special trust and confidence*. However, the headquarters company commander called me, inquiring about my plan to address the issue. I wondered why he was questioning my functional role. He oversees the morale and welfare of the Marines in the company but does not have direct responsibilities as a functional manager in my section.

Moreover, he would not be accountable for any of my shortcomings. So, I asked him, "Why are you concerned with item 'X's' readiness?" The reporting process seemed ambiguous, and this confusion grew because those involved in the MS did not seem to grasp their "clearly" defined roles. He responded, "Because the battalion executive officer asked me." This response introduced a new uncertainty: was I expected to continuously update the headquarters company commander on my progress as a functional manager?

The reporting process seemed ambiguous, and this confusion grew because those involved in the MS did not seem to grasp their "clearly" defined roles.

Example 2

I once worked in an organization that layered one MS over another. Like an infantry battalion, all functional managers fell under a headquarters company. However, unlike an infantry bat-

talion, that headquarters company fell within a headquarters battalion. This company reported to a battalion commander who answered to the regimental commander. The headquarters and the battalion commander sought authority over the functional departments for management and product quality control. However, functional managers reported directly to this organization's regimental commander, bypassing the administrative roles of the headquarters and battalion commanders. This structure quickly became dysfunctional due to the confusion of a perceived dual chain of command, leading to ambiguity, stress, and role conflicts. Many grappled with the question: *Who do I work for?* In this case, it took 90 days to clarify that my direct superior was the regimental commander, not the headquarters battalion commander, as initially assumed.

The layered MS aimed to support the regimental commander's role, supporting the functional managers. This role centered on serving the Marines, encompassing morale, motivation, mental and physical readiness, and annual training. However, this became counterproductive, as the battalion's role often clashed with the functional departments. The term "bureau pathology" describes this situation, where "the dual lines of authority reduce the tendencies of department members to become so busy protecting their little worlds that the organization's overall goals become secondary."[2] Daily conflicts arose between the functional departments and the layered MS structure. For instance, operations would halt for annual training seminars, with the company commander expecting total attendance, even if it disrupted mission preparations. This narrow view overlooked the extensive practice required by functional departments.

I frequently clashed with the company commander, who acted on the battalion commander's intentions. Meanwhile, I followed the direct guidance of the "regimental" commander, my immediate superior. I was in a position that required me to align with conflicting priorities. This tension peaked within 21 days of a new battalion commander taking charge. The battalion commander relieved me due to my role conflict with the headquarters company commander. I then Requested Mast finding it unjust to be dismissed by someone I did not directly report to. However, the regimental commander intervened before the Request Mast could proceed and resolved the issue.

Looking back, I see this as a power struggle between me, the functional manager, and the "production managers" (headquarters and battalion commanders) whose primary goal was to serve the Marines. The root of the conflict lay in the blurred lines and lack of unity of command caused by the layered MS.[3]

Moving Forward: Making the Inevitable Military MS Work

Matrix structure offers many benefits to our organization, but leaders must actively address and prevent potential issues to reap these benefits. One notable weakness of MS is the inherent power struggle within its structure. Paul R. Lawrence suggests methods to address and mitigate these issues.[4] The top manager or commanding officer must punish combative competition decisively. Competition arises when each party tries to gain an advantage, leading to occasional imbalances and fostering a hostile culture. Stanley M. Davis and Lawrence recommend educating leaders in MS about the dual command structure and clarifying expected roles and their execution.[5] If imbalances persist, both parties suffer. Matrix structure leaders should aim to transform conflicts into constructive outcomes while maintaining an institutional perspective. They should remove MS managers who, due to their weaknesses, cause significant setbacks. As Davis and Lawrence suggest, stronger leaders should replace these weak leaders.[6]

Another strategy for success in a matrix organization involves incorporating emotional intelligence.[7] Given that goals in MS can sometimes misalign, emotional intelligence can offer a more effective support structure than mere force. Research indicates that emotionally intelligent individuals can better align goals in matrix organizations by managing and reducing unproductive emotions that hinder collaboration.[8] In the future, to ensure the successful implementation of an MS organization, it is essential to provide specialized education on its structure and to prioritize the inclusion of emotionally intelligent leaders within the MS framework.

Matrix structure offers many benefits to our organization, but leaders must actively address and prevent potential issues to reap these benefits.

Notes

1. S.P. Robbins, and T.A. Judge, *Organizational Behavior*, (Upper Saddle River, 2009).

2. Ibid.

3. S.M. Davis, and P.R. Lawrence, "Problems of Matrix Organizations," *Harvard Business Review*, 1978, http://web.a.ebscohost.com.ezproxy.liberty.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=b8bc9e0f-7bd6-466bafce-292169df48ed%40sessionmgr4006&hid=4206.

4. Ibid.

5. Ibid.

6. Ibid.

7. ST. Sy and S. Cote, "Emotional Intelligence: A Key Ability To Succeed in the Matrix Organization," *The Journal of Management Development 23*, No. 5/6 (2004).

8. Ibid.

Subduing the Enemy Without a Fight?

The limits of cognitive warfare

by 2ndLt Paul Shields

With the development of digital applications, social media, and technology, there is a growing sentiment that shaping digital information may prove to be decisive in competing against peer adversaries. Yet, how influential can we be in this domain? This article will examine the limits of one particular method of information warfare highlighted in *MCDP 8*: the Cognitive Indirect Approach.[1] By cognitive, we mean aiming messages to directly influence our opponent's thinking processes. The intent is to use information to bend our opponent's perceptions, decision making, and ultimately their will to compete or fight. The cognitive thus focuses on the human element, whereas a "functional" approach uses information to influence non-thinking processes, such as a weapons or supporting system.[2]

To give an example, consider Russia's ongoing text campaign against Ukraine. As early as 2014, the Russian military bombarded Ukrainian soldiers with texts to their private cell phones, threatening their families and friends while demanding surrender.[3] The intent of these messages is to generate confusion, lower morale, or increase doubt in the mission or cause. In theory, this allows an indirect say over what and how the enemy thinks, with the hope of exploiting their mental and moral factors.[4] In short, it is classic propaganda.

The cognitive approach is attractive in theory. If taken to the extreme, it suggests we might be able to wholly achieve our objectives using non-kinetic means. With just the right sounds, images, and phrases we can get our enemy to put their guns down without having to lift our own. It argues for winning a war and securing peace without firing a weapon. It echoes Sun Tzu's saying, "Supreme excellence consists in breaking the enemy's resistance without fighting."[5]

>2ndLt Shields is a Logistics Officer, currently serving as the Assistant Logistics Officer for 3/6 Mar.

Although *MCDP 8* argues "human cognition is highly susceptible to manipulation and deception,"[6] social science research demonstrates the exact opposite. Much of the current misinformation narrative depicts humans as profoundly gullible, routinely revising their worldviews and behaviors based on what they encounter online. Yet, contrary to this conventional thinking, individuals are stubborn and difficult to influence. As a result, both our fears and interest in people's manipulability are largely unfounded. There are thus clear limits to the kinds of cognitive effects we might hope to achieve in an information environment. In particular, scholars who communicate with populations in China and Russia cast doubt on the ability to influence and change thoughts directly through digital efforts. Not to mention, it is almost impossible to accurately measure information effects on the cognitive level.

The Wide World of Cognitive Effects

The field of propaganda studies can help us better understand cognitive effects, as the literature is extensive, well-developed, and constantly evolving. Moreover, given the saturation of information technology in daily life, scholarship on misinformation has exploded in the last decade. For our purposes, we can begin with three general theories: indoctrination, signaling, and agenda setting.

Indoctrination is the standard brainwashing theory.[7] It suggests information goes directly to the brain, is absorbed, and then directly produces attitudes, feelings, and behaviors similar to the message content. If someone watches a music video that demonstrates positive feelings about Xi Jinping, the consumer of the message learns to love the Chinese dictator. This theory is demonstrated at the end of Orwell's 1984 when Winston, the protagonist, becomes brainwashed into finally loving Big Brother. What this theory incorrectly assumes is that people's opinions reflect the information they consume. And just because someone watches Chinese state television, as an example, they must believe what they watch and hear. However, in reality, humans are complex and have a wide range and, often, a complacent response to digital information. We are influenced by a wide variety of inputs that form opinions and responses based on where we were raised, our family life, and our education level, not just the media we consume.

Social scientists have noted that in countries like China and Russia, digital propaganda often does not result in persuasion.[8] Signaling theory argues that information can even have the opposite cognitive effect of its intention. In studies on Chinese and Russian

populations, a great deal of messaging from their government (although endowed with massive resources and totalitarian control) is unpersuasive and even counterproductive.[9] In fact, one observed effect of Chinese propaganda is to have their population be so off put by the heavy-handed messaging they feel cynical.[10] It can be easy to think that information messaging is straightforward—that it is simply swallowed by consumers. Yet, people from totalitarian societies often perform their allegiance as a way to simply get by. Controlling what is publicly said does not mean controlling what is thought privately.

The theory of agenda setting also demonstrates unconventional ways in which information campaigns are waged. While information might not be convincing, it can be used to crowd out mental space. Perhaps we have all experienced cognitive overload after spending hours online, as a deluge of information fogs our ability to think. Using the right channels, narratives that are relentless and repetitive can come to dominate alternatives. A novel study out of Harvard finds that the Chinese Communist Party monitors and tailors hundreds of millions of social media posts for purposes of distraction.[11] Through constant oversight, the Chinese Communist Party blocks arguments and skeptical views of the government. Controversial issues appear nonexistent to Chinese viewers online. In Russia, something similar is happening, though, through traditional media channels. Inside Russia, the popular Kremlin-controlled media determines the salience of issues for Russian viewers while deliberately ignoring news about key opposition figures that challenge Putin's government.[12]

A Different Approach

What this research suggests is that while a commander's intent with information may be clear with a defined task and purpose, what is actually achieved is never fully determined. Again, consider Russia's aggressive text campaign against Ukraine. When Ukrainian soldiers are interviewed about the possible effects of the texts attempting to break their will, the results are mixed, if inconsequential at best.[13] Some say it bothers them, lowering their morale. Others claim it motivates them and boosts their will to fight. It may be that the effects of the campaign are diverse and sometimes counterproductive, yet it is unclear how it translates to action on the battlefield.

Moreover, our framework in *MCDP 8* limits our understanding. Reading *MCDP 8* leads to the conclusion that information should be treated the same as fires: "Fires include the collective and coordinated use of any capability that can create physical (functional) or cognitive effects on the target or system."[14] While this may be true for functional effects like jamming a radar system or

intercepting communications, it begins to be more ambiguous in the cognitive domain. Accurate fires implies precision, identification, and measurability. But information effects in the cognitive domain are often unpredictable. Humans are limited cognitive processors who rely on accessible pre-established ways of thinking to navigate their environment.[15] We are often blind to external influences. This fact runs counter to the idea of information functioning as fires on the cognitive level. Indeed, distributing information may be a science, but the world of messages, rhetoric, and communication, and how it is to be understood, is an enigmatic art.

Social science argues the best way to understand messaging and information effects is whether they *reinforce* or *degrade* existing and or latent feelings. This framework understands that target populations are not blank slates. People develop opinions over the years and carry a wide range of knowledge and experience. Thus, information nudges pre-existing attitudes in a certain direction.[16] In other words, we do not convince anyone of anything. Rather, preconceived ideas are either strengthened or weakened. This indicates that for messages to be effective, we must first have a deep understanding of the audience and where they stand on key issues and decisions. Additionally, information campaigns must be highly targeted and sent through trusted channels. The more specific a message can be to an individual, the higher the likely effect of either reinforcing or degrading a prior-held belief. Ultimately, understanding the audience is important. It sets limits on what is possible. You do not find audiences for your message. You find messages for your audience.

This alternative understanding argues that information doesn't work to change attitudes, but rather serves more to reinforce predispositions in an audience.[17] In this regard, I would argue that our language of information "effects" in the cognitive domain should change. It might be trivial, but it should be one from *effect* to one of *activation* when it comes to *MCDP 8's* "Cognitive Indirect Approach." Information activates certain beliefs. Information activates an enemy's way of thinking. Information activates negative views of their leadership. This better captures the reality of how digital information shapes our thinking.

Against Over-investment and Over-reliance

Russia's war on Ukraine has reminded us of the fact that the leader's will and public opinion are important in influencing a war's outcome. Yet, we struggle with the fact that there is no satisfactory way to completely measure human group responses to information. The realized effects of information campaigns through digital means are often scientifically immeasurable. This does not completely rule out information operations. Operations in information dissemination, deception, and simulation are as old as war. Playing upon the opponents' thinking process to deceive intentions and capabilities is fundamental to strategy in combat.

Rather, we should take what is understood in the business world: we cannot know how influential marketing campaigns are, yet we continue to pursue them because there might be potential. We can both recognize the limits of our cognitive-indirect approach and still have it as a part of our toolbox.

In summary, when it comes to information warfare in the cognitive domain, the evidence argues against over-investment and cautions against over-reliance. The research runs counter to the assumption laid out in *MCDP 8*: that humans are easily deceived and manipulated. Our audiences are much smarter and more independent than we would like to admit. We must understand what realistic effects are possible and how diverse, inconsequential, and even counterproductive they may prove to be. We must also accept that our efforts may not lead to direct tangible outcomes. Surely, information that targets the cognitive domain will continue to be integrated into operations, but Sun Tzu's fantasy of "winning without a fight," is just that, a fantasy.

Notes

1. Headquarters Marine Corps, *MCDP 8, Information*, (Washington, DC: 2022).

2. Ibid.

3. Raphael Satter and Dmytro Vlasov, "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts," *Associated Press*, May 11, 2017, https://apnews.com/article/technology-europe-ukraine-only-on-ap-9a564a5f64e847d1a50938035ea64b8f.

4. *MCDP 8, Information.*

5. Sun Tzu, *The Art of War* (Chichester: Capstone Publishing, 2010).

6. *MCDP 8, Information.*

7. H.D. Lasswell, "The Theory of Political Propaganda," *American Political Science Review* 21 (1927).

8. H. Huang, "The Pathology of Hard Propaganda," *Journal of Politics* 8, No. 3 (2018).

9. Paul Shields, "Killing Politics Softly: Unconvincing Propaganda and Political Cynicism in Russia," *Communist and Post-Communist Studies* 54, No. 4 (2020).

10. "The Pathology of Hard Propaganda."

11. Gary King, Jennifer Pan, and Margaret Roberts, "How Censors in China Allows Government Criticism but Silences Collective Expression," *American Political Science Review* 107, No. 2 (2012).

12. A. Kazun, "Agenda Setting in Russian Media," *High School of Economics Research Paper* 49, (2017).

13. "Ukraine Soldiers Bombarded by 'Pinpoint Propaganda' Texts."

14. *MCDP 8, Information.*

15. Rodney Brooks, "Intelligence Without Reason," *Computers and Thought* 1293, (1991).

16. Garth Jowlett and Victoria O'Donnel, *Propaganda and Persuasion, 2nd ed.* (Newbury Park, CA: Sage, 1992).

17. Ibid.

GALVION™

PURPOSE-DESIGNED PURPOSE-BUILT

MARINE-READY

OPTIMIZED STABILITY. SCALABLE POWER MANAGEMENT.
CLEAR FUTURE TECHNOLOGY PATH

Galvion's ground-up, customized Integrated Helmet System (IHS) solution designed for the United States Marine Corps, with direct Marine feedback.

More ballistic coverage, better fitting with maximum stability, scalability and comfort. Built to deliver enhanced Marine operational capability and through-life value.

Easy integration with current USMC equipment, including Hearing Protection, SBNVG and ECOTI, and a clear path for integrating evolving technology.

WWW.GALVION.COM

Hyperscale Cloud Services for Marine Corps Operations

Navigating the complex landscape

by LtCol Christopher Tsirlis

>LtCol Tsirlis retired from the Marine Corps in 2022 after 31 years of faithful service. He has served in numerous operational commands and several MAGTF communications-related billets. His last tour was as the Commanding Officer of Marine Wing Communications Squadron 28. In his civilian capacity, he worked as a Product Solutions Manager for Gaming, Exercising, Modeling and Simulation for Microsoft Corporation, and now recently works for Airbus Corporation, U.S. Defense & Space Government Solutions, as the Vice President of Business Development and Product Innovation for Advanced Satellite Ground Systems located in Plano, TX. The thoughts and opinions in this article are his own.

The art of warfare is a symphony of synchronized combat power, an intricate harmony of countless organizational dependencies and interdependencies, more akin to an orchestra than a rock band. Just as music demands skill and human cognition to create a melodious tune, military operations rely on human judgment, leadership, and courage in conjunction with advanced technologies. The top technology trends in 2024 all lean heavily on hyperscale cloud services, in particular, artificial intelligence (AI).[1] This siren call of hyperscale cloud services beckons the Marine Corps along with other military branches with promises of technological advancement, cost-efficiency, and flexibility. However, will it make the Marine Corps stronger and more lethal? Beneath this alluring marketing façade lies a complex web of implications that must be thoughtfully considered. This article delves into the multifaceted implications of embracing commercial hyperscale cloud services for military operations, emphasizing the importance of striking a prudent balance and a skeptical eye on the risks. It also focuses on where to weigh our investments to ensure we maintain flexibility going forward.

Overreliance on New Technology Trends

In the contemporary landscape, the commercial world's influence on military thinking has given rise to the belief that adopting business operating models for military processes can significantly enhance speed, efficiency, and mission effectiveness. This may or may not be true. As of late, what is touted most often is around cognitive decision making using AI/machine learning (ML) technologies. You will often hear terms like "decision superiority" or "decision advantage" bounced around as it relates to Joint All-Domain Command and Control (C2) concepts.[2] Does anyone really believe this is possible? Even with perfect information, decision makers get it wrong many times because logic and reason are also influenced by so many other factors such as fear, group thinking, and their own personal bias. More importantly, there is little consideration for "communication logistics" and what it means to install, operate, and maintain network services for pacing threats like China or Russia. As much as I would like to believe the marketeers and slogan sleuths about the need for more technology, we are introducing a complex web of interdependencies that will inevitably make the Marine Corps less flexible and less adaptable. Commercial tech companies are showing the benefits of their products but rarely expose what's under the waterline. Doing so often exposes what really are the corporate entity motives for the campaign of innovation that is so often heralded. Buyer beware.

While these technologies certainly offer unprecedented possibilities in data manipulation and synthesis, the Marine Corps must exercise caution and prudence in its blind embrace. An unwarranted rush to adopt these commercial (often managed) services without rigorous scrutiny, testing, and evaluation against organizational doctrine and key warfighting concepts may introduce unanticipated organizational friction. This friction can, paradoxically, detract from the military's core mission sets by fostering overconfidence in new and exciting technologies, introduce complacency in exercising sound military doctrine, or worse yet, our own hubris. It is critical to understand that

while modern technologies, including hyperscale cloud services, can indeed function as a force multiplier, they must always remain a tool, not a replacement for human judgment, leadership, and critical thinking. As much as there are advantages, adoption can introduce some disadvantages too.

Some glaring questions that come to my mind. Does the Marine Corps believe that our adversaries will not target the physical architectures these commercial hyperscale cloud services depend on? Are the Naval Services inadvertently tying their own hands by handing to commercial providers the critical data stores of the U.S. government for some strange belief that we will be better off with these commercial entities hosting this data? Is the Marine Corps making themselves more vulnerable and externally dependent on outside commercial entities for critical C2? Do we become more fragile or anti-fragile in our critical C2 infrastructure by trusting commercial entities? Our adversaries always get a vote and often will influence the answers to these questions.

In my view, the Marine Corps should not follow marketing promises or false assumptions nor trust commercial company claims about their products without a high degree of certainty they will act appropriately for national security. Operational guarantees are needed beyond simple legal contract/program language and strongly worded Service-level agreements. This is not good enough for Marines and sailors to bet their lives on. Let us not forget that when commercial enterprises fail, they simply file for bankruptcy protection, change some leadership out, and start the blame game. If the military fails, nations must sue for peace, which is usually on unfavorable terms. The Marine Corps has no-fail missions. At the end of the day, hyperscale cloud companies are not likely to expose their shareholders or employees to too much risk, even during times of war, and certainly not willing to risk their balance sheets for national security purposes. The incentives are neither good nor bad, just different, and the Naval Services need to really consider this before putting all their eggs in this commercial basket. This is something to be considered when it comes to handing over even some minor network service operational controls to them. The stakes are simply higher for the Marine Corps, and we must be very careful in any reliance that can create critical vulnerabilities for our adversaries to exploit.

Understanding Hyperscale Cloud Services

Before delving deeper into the implications, let us gain a more comprehensive understanding of hyperscale cloud services. These services encompass large commercially owned data centers that provide high-performance computing, storage, and networking resources over the Internet via multiple transmission mediums. They play an integral role in a wide range of applications, namely the latest craze: AI. Artificial intelligence, being computationally intensive and data-hungry, necessitates the kind of resources offered by hyperscale cloud services, particularly graphics processing units that enable these types of services. The advantages are many: infrastructure cost savings, security, scalability, and innovation for advanced network-aware applications to name a few.

Benefits of Hyperscale Cloud Services

Hyperscale cloud services provide a multitude of advantages if managed correctly:

- *Cost Savings:* The cloud services allow users to bypass the need for substantial investments in physical infrastructure. This not only reduces the initial costs but also alleviates the ongoing expenses related to maintaining and upgrading this infrastructure.
- *Scalability*: Users can readily adjust their cloud resources dynamically to meet their evolving needs. Most cloud services have flexibility which allows for seamless scaling up or down without the concerns of overprovisioning or underutilization. This is a great benefit for surge operations.
- *Flexibility:* With hyperscale cloud services, users have access to a wide array of cloud services and technologies. This flexibility enables them to choose the best-suited cloud services for their specific use cases or applications; however, in reality, each hyperscale cloud vendor is not incentivized to work in multi-cloud environments which conversely turns this into a disadvantage.
- *Innovation:* The cloud's potential for innovation is huge. The latest and most advanced technologies and ser-

MCSC talks cloud computing at Cloud Technology Summit. *(Photo by Jennifer Gonzalez.)*

vices are offered by cloud providers namely because of the benefits stated above. Innovators in the Marine Corps can leverage this environment for experimentation and the exploration of mission-related and novel solutions.

With this understanding, we can more clearly appreciate why military organizations are drawn toward hyperscale cloud services. However, as with any technical endeavor, there are significant risks and challenges that come hand in hand with these enticing benefits.

Risks of Hyperscale Cloud Services

Embracing hyperscale cloud services for military operations introduces significant risks, the foremost being the potential loss of control and visibility over sensitive data and applications. Trusting commercial providers to safeguard critical military data exposes the organization to various vulnerabilities outside of its operational and tactical control. Furthermore, the dependence on a limited number of cloud providers poses an additional risk. This dependency forces the military to align its operational needs with the hyperscale provider's capacity, potentially divergent interests, and quality of service. Such reliance on external entities for mission-critical operations creates a substantial vulnerability that requires careful consideration.

Of note, the Army has made the adoption of hyperscale cloud services part of its unified network plan for multi-domain operations.[3] Under their common services infrastructure, they seek to leverage globally assessable hardware and services to support data analytics to use AI/ML across the force. They clearly have evaluated the risks and believe a hybrid cloud architecture spread across strategic, operational, and tactical levels provides them with operational increases. Ideally, this will help them take advantage of cloud/AI-enabling technologies to support unified network communications.

The Marine Corps should tread lightly here before it dives too far forward. There is no proof yet that the Army is on the right track since they do not have real-world use cases to draw lessons from.[4] Yes, there is experimentation going on, but it is very scoped and limited in nature. I cannot help but think what this means operationally for those sailors and Marines who must run the network and then half to navigate not only the byzantine bureaucracy of the DOD but also the business interests of commercial hyperscale cloud providers. For each higher headquarters communications section, this will complicate operational plans if the services that are critical for day-to-day operations are hosted in the cloud.

- *Loss of Control and Visibility*: One of the primary concerns is the loss of control and visibility over sensitive military data. Military operations, by their very nature, demand an exceptionally elevated level of security, reliability, and resilience to safeguard sensitive information and ensure mission success. The use of hyperscale cloud services necessitates an inherent level of trust in the cloud provider's ability to safeguard this information while also adhering to the organization's specific requirements. However, this trust introduces the military to the peril of potential cyberattacks, data breaches, legal disputes, and regulatory violations. This also widens the aperture for insider threats within commercial entities. Moreover, the Marine Corps may not have full access to, or knowledge of, the physical location, configuration, performance, and status of the cloud infrastructure and services, limiting their ability to secure, monitor, audit, troubleshoot, and optimize their cloud operations. This may become problematic for Naval Services as they seek to adjust to enemy actions in realtime. No commander will have the authority to change cloud provider priorities. Farming out this risk must be balanced through a diversity of options available to the commander to operate and maneuver in the information space.

There is no proof yet that the Army is on the right track ...

- *Dependence on a Limited Few Commercial Providers:* Another significant risk revolves around the military's dependence on a limited number of commercial cloud providers, namely AWS, Google, and Microsoft being the largest players. Military operations demand rapid and agile adaptation to changing threats and environments. This is something that cloud providers say they provide. However, when using hyperscale cloud services, the military must rely on the cloud provider's availability, capacity, functionality, and quality of service. They also set their own priorities based on market conditions and not military necessity. This reliance can constrain the military's options and flexibility to meet its operational needs. Furthermore, cloud providers may have commercial, social, or political interests that diverge from or oppose the military's objectives.[5] For example, the cloud provider may prioritize its profitability over its customer's satisfaction, or it may cooperate with, or be influenced by, foreign adversaries or competitors. The Marine Corps must scrutinize the alignment of these incentives and contemplate the potential risks involved in entrusting its vital operations to organizations that may not share the same level of commitment to mission accomplishment.
- *Dependence on the Internet–Undersea Cable Security:* There are countless security attack vectors with hyperscale cloud providers. One of the most glaring ones is its dependence on commercial telecom providers. Undersea communication cables are at risk.[6] Our adversaries are growing in sophistication and exerting influence over telecom providers operating in their sphere of control or influence. Submarine cables are owned by combinations of private companies, state-owned firms, and international consortia from around the world; a single cable could have anywhere from one to dozens of owners.[7] Authoritarian governments like China may be able to influence state-owned telecoms to spy on cable landing stations and disrupt the flow of data during conflict. Any

manipulation of the global internet infrastructure can influence how the Marine Corps secures its vital communication paths. Cybersecurity has been the focus in recent years, but little investment has been made to secure the actual physical infrastructure that hyper-scale cloud providers rely on.

The Hyperscale Business Model

To fully grasp the implications of hyperscale cloud services, it is essential to understand the fundamental difference between two prevailing models: operational expenditure (OPEX) and capital expenditure (CAPEX). For the Naval Services, ask your local supply officer or procurement officer to buy network services like a cable television subscription. They may scratch their head for a while. Most do not have the expertise to facilitate this new consumption model that is presented to the Marine Corps. At the network enterprise level, this may make sense. However, for operational units, this is a huge change and challenge under the current fiscal procurement construct for communication planners.

OPEX Model

Hyperscale cloud providers operate on an OPEX model. This means they charge their customers based on their usage or consumption of cloud resources. Under this model, customers are not required to invest in or own any physical infrastructure or assets. Instead, they pay for the cloud services they use. This model offers several benefits, namely cost savings.

However, the OPEX model is not without its drawbacks and challenges for the Marine Corps:

- *Loss of Control and Visibility:* Customers must trust the cloud providers to safeguard their data and comply with their requirements. They may not have full access to or knowledge of the physical location, configuration, performance, and status of the cloud infrastructure and services. *It's in the cloud* may not be good enough for military operations and since the DOD has not ever passed an audit, the promised cost savings may not materialize as promised by cloud providers.[8]
- *Complexity and Unpredictability of Cloud Costs:* The Marine Corps must carefully monitor and manage their cloud usage and consumption, as they may incur unexpected or hidden charges from the cloud providers. Forecasting and budgeting cloud costs can be challenging.

CAPEX Model

Conversely, some customers may prefer or require a CAPEX model for their cloud needs. Under this model, they must invest in or own their IT infrastructure or assets, either on-premises or in a colocation facility. This is unlikely going to change because of the nature of distributed operations for the naval services. This model offers a distinct set of benefits:

- *Control and Visibility:* Maintain full ownership and responsibility over their data and applications hosted on their own IT infrastructure. They can also secure, monitor, audit, troubleshoot, and optimize their IT operations.
- *Independence from a Single or a Few Cloud Providers:* Customers are not dependent on the availability, capacity, functionality, and quality of service of any external cloud provider. They can align their IT objectives with their military objectives without being influenced by market, social, or political factors.
- *Predictability and Stability of IT Costs:* Customers can calculate and plan their IT costs based on their fixed assets and depreciation rates. They can avoid or reduce the variable costs associated with using cloud services.

However, the CAPEX model also presents its own set of challenges:

- *High Initial and Ongoing Costs:* Must bear the upfront and recurring costs of purchasing, installing, upgrading, and maintaining their own IT infrastructure. Training costs continue as well.
- *Limited Scalability and Flexibility:* Customers must estimate and provide their IT resources based on their projected needs and demands. Accessing or integrating with hyperscale cloud services or technologies may also be problematic.

These two contrasting models represent the dichotomy the Marine Corps must navigate when considering its cloud computing needs. While the OPEX model offers undeniable advantages, it also introduces risks and complexities that should not be. Moreover, the current CAPEX model, which is unlikely not going to change soon, while providing control and predictability, poses its own limitations, particularly in terms of scalability and innovation.

Dangers of Overreliance on AI/ML

The latest trend in the realm of technology, one that has generated a great deal of enthusiasm, is the use of AI and ML for algorithms to enable decision support. AI, as a branch of computer science, aims to create machines or systems capable of performing tasks that traditionally require human intelligence. The applications of AI are incredibly diverse, extending to fields such as healthcare, education, entertainment, transportation, and more. Most notable is the recent use of large-language models like ChatGPT. However, the adoption of AI in warfare comes with its own set of complex challenges and potential dangers that demand thorough consideration.

The train has left the station on the excitement large-language models have created for military planning. Using large-language models operational planners can save time and enable better understanding, but absent a trained user, relying solely on model-produced outputs risks confirmation bias. The more time the military spends on critical thinking and basic research methods while translating both into structured questions, the more likely large-language models are to help planners visualize and describe complex problems.[9] So it will be critical to be able to identify when AI-producing outputs begin to degrade decision making. Recent history of societal reliance on smart phones deduces that overreliance will naturally occur. When this happens, we will become less critical in thought and less discerning when it matters most in military affairs. Not good.

The Future Proliferation of AI

AI, with its capacity to enhance

every aspect of warfighting, will permeate all domains of military operations.[10] It is essential to recognize that while AI can bring significant benefits, it is not without its risks, particularly in military contexts. One of the most prominent concerns is the development and use of lethal autonomous weapons systems (LAWS).[11] These systems can independently select and engage targets without human intervention. While LAWS have the potential to increase the speed, accuracy, and efficiency of military operations, they simultaneously raise substantial ethical, legal, and moral concerns. LAWS may lack the essential attributes of human judgment, accountability, and empathy when making life-and-death decisions on the battlefield. Their operation can present challenges in adhering to the laws of armed conflict and ethical norms, potentially leading to violations and the erosion of moral standards.

Considerations of Using AI in Military Operations

Beyond the legal and ethical concerns listed above, the integration of AI into military operations introduces both potential benefits and significant risks. The capabilities of AI systems, with their capacity for faster information processing, decision making, and action execution, are undeniable. However, they also introduce uncertainty, complexity, and unpredictability into warfare. Consider the following:

- *Autonomous and Unpredictable Behavior:* AI systems may exhibit autonomous and unpredictable behaviors, particularly in complex or uncertain situations. They may bypass human commands or intentions, raising concerns about their reliability and predictability in the heat of battle. A poorly trained AI model can lead to disastrous outcomes. If that occurs, trust in these systems goes out the door.
- *Generation of False or Misleading Information:* AI systems may inadvertently generate false or misleading information or analysis, which can affect human perception and judgment. Especially if these systems are being used for wargaming activities or operational planning. They are also vulnerable to zero-day cyberattacks like any other information system. This becomes a crucial concern in scenarios where AI plays a significant role in decision making.
- *Introduction of Vulnerabilities:* AI systems may introduce new vulnerabilities and asymmetries in military operations, which can be exploited by adversaries or competitors. The full attack vector for cyber attackers is not fully known.

Considering these challenges, it is imperative to consider potential safeguards and norms to govern the use of AI in warfare. One approach involves the establishment and adherence to ethical principles and standards for the development and deployment of AI systems. However, it is essential to remain pragmatic about the application of these principles. In the context of warfare, ethical principles may not be as straightforward to apply as they are in civilian domains. There is little doubt that adversaries like China and Russia do not hold the same ethical principles and will not hesitate to develop AI technologies with Western norms in mind.

Rather than tying AI to a rigid set of ethical principles which is a human endeavor, the focus should remain centered on mission-critical objectives for combat operations. While ethical considerations and legal frameworks remain paramount, the primary concern should be that AI systems are transparent, accountable, dependable, and can be verified, validated, and assessed for their success in the mission. The emphasis should not solely be on aligning AI with human values, as this can be a challenging endeavor, particularly in the context of military operations. If enabling technology can help us dominate and win in combat, then we must leverage it.

A fundamental principle that should underpin the use of AI in military operations is the retention of human control. This principle dictates that human operators or supervisors should have the authority, responsibility, and capability to monitor, intervene, or override AI systems when necessary or appropriate. Moreover, human operators or supervisors should receive adequate training, education, and awareness of the capabilities, limitations, and risks of AI systems. Human control ensures that AI systems remain a valuable tool that complements human judgment and leadership, rather than replacing it.

Becoming Anti-Fragile

Will the growing reliance on hyperscale cloud and AI/ML services make the Marine Corps more fragile? It may just do that. As the military landscape continues to evolve in the 21st century, the concept of antifragility has emerged as a crucial consideration.[12] Antifragility entails more than just surviving shocks and disruptions; it involves harnessing these challenges to become stronger and more resilient. For example, our IT industrial base, the network of suppliers providing goods and services to the military, faces increasing risks, operational readiness, effectiveness, and resilience hang in the balance and therefore very fragile. A high-end attrition fight with a near-peer enemy will expose these vulnerabilities, which can have dire consequences during a long campaign.

In my view, decision makers need to ask the fundamental question, will a growing reliance on hyperscale cloud services like AI make them stronger or weaker? What are they giving up both physically and temporally in their forces? What interdependencies must come together to ensure this growing reliance does not cause a significant crash at the worst possible times?

Continued adaptation through experience of iteration of decision making is key for Marine leaders to hold on to. If the Service seeks to offload cognitive functions to AI algorithms, then individual and institutional cognitive power will decline over time. There needs to be some tempering of the notion that we *need AI* to survive the next fight. The war drums sung by tech companies keep feeding this narrative to the DOD. That so-called critical need may, in fact, be drawing the Marine Corps into a mental and cognitive ambush underwritten by the belief that the speed of decision making through machines will increase quality decision making and outcomes.

Commercial and governmental entities keep beating this drum. This is a dangerous proposition and dehumanizes what are inherently human qualities in leadership and warfare. Hyperscale cloud/AI technologies may not make us more resilient or lethal. In my view, it certainly does not create antifragility in the Marine Corps due to its many external dependencies. Let us not be naïve and forget what the real incentives and financial motives of commercial entities really are. The Marine Corps must be pragmatic and recognize what is hype and what is not.

I do advocate continued exploitation of opportunities by experimenting with innovative ideas, technologies, and strategies. Embracing innovation is essential to meet the ever-changing landscape of warfare if it enhances diversity and redundancy in the systems involved in naval warfare. Too much faith in technology can often mask larger organizational problems. Having multiple options, pathways, and resources ensures that the Marine Corps can weather disruptions and shocks to their network services effectively.

Hybrid Adaptive Networks

In determining where to weigh one's efforts on technology, I suggest that a strong resilient software-defined network is the best approach. To mitigate the significant risks and challenges posed by an overreliance on hyperscale cloud services, the Marine Corps and other military branches should highly invest in alternative or complementary approaches. One such approach is the utilization of hybrid adaptive software-defined networks, specifically those that rely on satellite communications (SATCOM) transport paths. Software-defined networking elevates network traffic management away from hardware with next-generation software, often in the cloud, for enhanced agility, control, and visibility. These networks possess the unique capability to roam seamlessly across multiple satellite and terrestrial networks. They create an end-to-end communications solution, offering flexibility, redundancy, and resilience, even in highly contested environments. A hybrid network leverages multiple transportation routes (celestial and terrestrial) to critical data stores or processing nodes.

The Marine Corps must earnestly leverage geostationary, middle-Earth orbit, and low-Earth orbit satellite capabilities to be available to sailors and Marines both at the halt and on the move, which will require ruggedized end-user devices and systems that facilitate mobility throughout the battlefield. There must be a stronger look at a much higher amount of SATCOM connections with virtualized waveforms being a top requirement for ensuring security. Ideally, the Marine Corps must automate its primary, alternate, contingency, and emergency plans in such a way that

it can dynamically maneuver the spectrum and route to ensure it has access to its data stores, both on-prem and in the cloud if need be. Multiple satellite constellations and a way to manage communicating with several constellations simultaneously to ensure there is resiliency through diversity. This is an example of technological anti-fragility which turns potential shocks to the network into operational strengths.

Using hybrid adaptive networks with muti-orbit, muti-frequency SATCOM capabilities offers many advantages for Marine Corps operations. Enhanced connectivity, especially in remote or denied areas where terrestrial networks might be unavailable or unreliable. Specifically for Marine Corps stand-in forces executing enhanced advanced base operations. This is essential for survival inside the enemy's weapons engagement zones. Operations inside the weapons engagement zones will require mobility and transport optionality for continued survivability. This will also increase control and visibility over critical data and applications.

Conclusion

The seductive allure of hyperscale cloud services in military operations conceals a complex and multifaceted landscape. There is a lot to consider, and it appears that the Marine Corps should be cautious in moving too fast. While these cloud services present undeniable benefits, including cost savings, scalability, and flexibility, they also harbor significant risks. The loss of control and overdependence on external commercial providers with potentially divergent interests are among the foremost concerns.

The integration of AI/ML, particularly in the form of lethal autonomous weapons systems, raises a new set of ethical and operational challenges. To navigate this complex terrain effectively, the Marine Corps must carefully consider the alignment of AI systems with mission-critical objectives. Focus should be placed on transparency, accountability, and reliability. Most of all lethality.

The fragility of an overall reliance on technology is concerning, especially of the nation's industrial base poses a critical concern, as it directly impacts operational readiness and resilience for technology sustainment. In an era marked by dynamic and complex challenges, the Marine Corps must endeavor to become antifragile, harnessing disruptions to become stronger and more adaptable.

To mitigate these risks and challenges, alternative approaches, such as hybrid adaptive networks that utilize SATCOM muti-orbital constellations, should become a staple of naval services' network topologies. These hybrid networks provide enhanced connectivity, mobility, survivability, and reduced dependence on only a few commercial providers, thereby addressing some of the most significant concerns associated with hyperscale cloud services.

In the end, while technology and hyperscale cloud services can be valuable tools, they should always complement and enhance the capabilities of military forces, rather than replace the indispensable qualities of human judgment, leadership, and critical thinking. Striking the right balance between these technological advancements while maintaining human-centric strategies is the key to addressing the challenges posed by the lure of hyperscale cloud services and AI in military operations. This careful equilibrium will define the success and resilience of Marine Corps C2 in the ever-evolving landscape of modern warfare.

Notes

1. Esther Smith, "Gartner's Top 10 Strategic Technology Trends for 2024," *Tech Republic,* October 23, 2023, https://www.techrepublic.com/article/gartners-top-10-strategic-technology-trends-for-2024/#:~:text=Gartner's%20top%2010%20strategic%20tech,AI-augmented%20development.

2. Terrence O'Shaughnessy, "Decision Superiority Through Joint All-Domain Command and Control," *Joint Force Quarterly 99, No. 4 (2020).*

3. Department of the Army, The Army Unified Network Plan Enabling Multi-Domain Operations, (Washington, DC: 2021).

4. Ashley Roque, "No Convergence in 2023: Army Deliberating the Path Ahead for Signature JADC2 Exercise," *Breaking Defense,* February 8, 2023, https://breakingdefense.com/2023/02/no-convergence-in-2023-army-deliberating-the-path-ahead-for-signature-jadc2-exercise.

5. Daisuke Wakabayashi and Kate Conger, "Google Wants to Work with the Pentagon Again, Despite Employee Concerns," *New York Times,* November 3, 2021, https://www.nytimes.com/2021/11/03/technology/google-pentagon-artificial-intelligence.html.

6. Justin Sherman, "The U.S. Should Get Serious About Submarine Cable Security," *Defense One,* September 13, 2021, https://www.defenseone.com/ideas/2021/09/us-should-get-serious-about-submarine-cable-security/185325.

7. Ibid

8. Ellen Mitchell, "Defense Department Fails Another Audit, But Makes Progress," *The Hill,* November 17, 2022, https://thehill.com/policy/defense/3740921-defense-department-fails-another-audit-but-makes-progress.

9. Benjamin Jensen and Dan Tadross, "Low Large-Language Models Can Revolutionize Military Planning," *War on the Rocks,* April 12, 2023, https://warontherocks.com/2023/04/how-large-language-models-can-revolutionize-military-planning/#:~:text=The%20large-language%20model%20helped%20military%20planners%20see%20battlefield,infrastructure%20investments%20like%20China%E2%80%99s%20Belt%20and%20Road%20Initiative.

10. David Vergun, "Artificial Intelligence Key to Maintaining Military, Economic Advantages, Leaders Say," *DOD News,* April 9, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2567486/artificial-intelligence-key-to-maintaining-military-economic-advantages-leaders.

11. Congressional Research Service, "International Discussions Concerning Lethal Autonomous Weapon Systems," *CRS Report,* August 16, 2019, https://crsreports.congress.gov/product/pdf/IF/IF11294/1.

12. Dana Kilsanin, "The Antifragile Mindset," *Psychology Today*, March 16, 2020, https://www.psychologytoday.com/us/blog/digital-altruism/202003/the-antifragile-mindset.

USAA®

8 MONEY MOVES TO MAKE WHEN YOU'RE NEW TO THE MILITARY

Virtually all military operations begin with some sort of detailed planning process. That same approach will help you get off to a good start with your personal finances. Here are eight money moves to make during your first few years of military service. Even if you're not new to military life, these tips serve as a great foundation for everyone's finances.

BUILD A BUDGET

The first step to managing your money is developing a detailed list of what comes in and a plan for what goes out. A good starting place is with a 20-50-30 budget.

- 20% spending and debt repayments
- 50% needs
- 30% wants

Start here, then personalize it to your individual needs and situation.

SAVE FOR EMERGENCIES

Set money aside in a savings account for the unexpected. Start with an initial goal of $1,000, then build until you can cover three to six months' worth of expenses.

CONSIDER THE TSP

The Thrift Savings Plan, also known as TSP, is the military's 401(k). It's a great place to start as you begin your retirement savings journey. When eligible, those under the Blended Retirement System are offered matching contributions, which is free money.

GUARD YOUR CREDIT

Your credit report and accompanying score are important. Start by using credit responsibly and always pay on time. Don't borrow what you can't pay back by the end of the month. Since military members are 76% more likely than other adults to report that an identity thief misused an existing account, take practical steps to safeguard your credit and identity.

These four tips are just the beginning. Follow this QR code or select this link to learn more about these in more detail and review the rest of the list.

Challenges for Military Aerospace

The annual global aerospace summit

by Maj Timothy Warren

From 11–13 September, the U.S. Chamber of Commerce hosted its annual Global Aerospace Summit, convening leaders from across industry, several governments, and media to discuss the future of and challenges facing all things aviation and space. With over 1,200 attendees and over 120 speakers, the 2023 summit proved to be the largest yet. Attendees heard firsthand perspectives on the state of aerospace from CEOs of major and moderate airlines, aerospace logistics organizations, and aerospace entrepreneurs, as well as five U.S. House Representatives, three Senators, twelve Federal agency and department leaders, one state governor, and the Space Force chief of staff. Notably absent were any uniformed representatives of the Army, Navy, Air Force, or Marine Corps to observe and record the event.

Plenty of topics during the seventeen hours of programming foretold both challenges and opportunities for military aviation. The most pressing topics that will affect the military's ability to compete in the aerospace ecosystem in the near term are the relatively easy access to space for many organizations, the looming boom of commercial unmanned vehicles, workforce shortages, and supply chain constraints. While these issues are already impacting the civilian market, military aviation will need to pay closer attention to these issues given its higher standards for recruitment, procurement, and security.[1]

Space

The topic of state and non-state organizations achieving relatively easy access to space was a recurring topic during the Summit's Space Day. Even without robust space programs, these organizations present new challenges to the DOD's ability to conduct global operations. Some capabilities that organizations could easily (for the right amount of capital) acquire in space include advanced communications, a wide range of observation capabilities with spotting artillery firings and impacts (forest fire spotting satellites being one specifically mentioned capability), and the ability to use one spacecraft to reposition satellites and other spacecraft.[2] Many of these capabilities previously belonged only to a select few state actors but are now at the disposal of our allies and adversaries. While the Space Force, along with other government and commercial partners, face these challenges, the entire Joint Force should be aware that future conflicts will extend beyond our atmosphere.

Summit presenters discussed at length the protection of U.S. and allied flagged space assets, both government and commercial. This includes the space just above Earth and future assets out to the Moon and Mars. The growth of the commercial space industry promises to boom in the coming years, and the United States, China, other nations, and private organizations are all eying deep space and lunar development for commercial purposes.[3] Some commentators have posited that space-based commercial assets could come into conflict with each other and—in a worst-case scenario—threaten to pull nations into conflict and pull terrestrial conflict into space and beyond.[4] The concept of space warfare is no longer the stuff of science fiction: the Joint Force needs to ensure that its space-based defensive planning and procurements are maintaining pace with the growing interests and threats in that sector.

Air

Many concerns and advancements in civilian aviation were discussed during the Summit's Aviation Day that will strain and challenge military aviation in the coming decade. Electric vertical take-off and landing vehicles are here, they are gaining certification, and they are not going anywhere; the same is true for all types of unmanned aerial vehicles. Many of these vehicles are artificial intelligence/remotely piloted and can serve as aerial taxis or aerial privately owned vehicles.[5] These emerging technologies present a world of advantages for civilian and military life, but they are also a safety and surveillance concern for our military facilities. It is only a matter of time before on-base residents will be delivered to their domiciles in electric vertical take-off and landing while other residents will have their groceries delivered via a drone. Even if these vehicles are not allowed on bases, many military airfields border major civilian population centers. This increased traffic near approach patterns will greatly increase the potential

>Maj Warren is a Commandant of the Marine Corps Fellow at the U.S. Chamber of Commerce who holds MOSs as an Aviation Logistician and Training and Education Officer.

for airborne mishaps. The addition of these private aerial vehicles will also allow adversaries new vantage points to observe and sense force postures while home and aboard. There are some in the military and Federal Aviation Administration already combating these risks, but the problem set is about to explode over the next decade.

Other safety concerns that were discussed that are crucial for military aviation included the growing shortage of civilian air traffic controllers and airfield infrastructure around the country. With a large percentage of annual military flight hours being earned into and out of civilian airfields, it is easy to see why the shortage of civilian air traffic controllers is a concern.[6] This problem is on top of the fact that the Federal Aviation Administration just seated a Senate-confirmed administrator after a year-plus gap and no new Federal Aviation Administration authorization passed into law. Furthermore, there were discussions involving the aging infrastructure at many airports around the country. There are efforts underway across the country to modernize many airfields, but the shortage of capital may keep the updates from maintaining pace with natural deterioration.[7] All these issues should be discussed by Service aviation leads and risk-mitigated by aircrew prior to flights away from home stations.

A shortage of pilots, maintenance personnel, and challenged supply chains were also mentioned at length during the summit. While most of the major airlines are not having issues hiring new aircrew, the same cannot be said for smaller or regional airlines. There is talk of extending the required airline pilot retirement age from 65 to 67, but this is only a temporary fix.[8] The same problem was mentioned about air traffic controllers, qualified aircraft maintenance personnel, and manufactured aircraft parts workers. The lack of maintenance personnel at airfields adds to the aircrew problem while the lack of qualified manufacturers further constrains

There are efforts underway across the country to modernize many airfields, but the shortage of capital may keep the updates from maintaining pace with natural deterioration.

aviation supply chains.[9] Additionally, the need to find sub-manufacturers who are reliable over the next few decades is becoming a growing concern, especially with the fact that China produces a very large number of subcomponents in the aviation industry.[10]

The reason these issues are concerns for the military will surprise no one. First, the military will recruit aircrew and maintenance personnel from the same pools as civilian companies. With recruiting already a challenge, the military needs to find *more* ways to recruit and retain quality personnel. One major airline mentioned a program that allowed any employee (or their family) who had been employed by the company for two or more years in any position to test for and then train to become a pilot (other airlines have similar programs).[11] This program has resulted in an increase in new pilot hires and increased pilot retention for the company. This process sounds like a warrant officer track that only the Army uses for new pilots and a program that other branches could adopt.

Civilian aviation supply chains have been constrained for a while now, and there are concerns that will also have effects on military supply which has much higher requirements for where certain parts and sub-parts can be manufactured. As the few aerospace component-producing companies run low on critical subcomponents, they will limit who can purchase certain parts, their prices will skyrocket, or a combination of these or other consequences.[12] Military aviation logisticians and acquisition personnel should look at how they are going to repair and resupply aircraft now and over the next decade or they risk giving adversaries a significant advantage in mission-capable aircraft.

Finally, sustainable aviation fuels, electric propulsion, and electric ground support equipment are emerging and will be on many airfields soon.[13] There are three reasons why these emerging technologies are going to be important for military aviation. First, the DOD needs to decide when/if they are going to invest in the next generation aircraft that will operate on sustainable aviation fuels or electric propulsion. Secondly, there is no infrastructure on modern military airfields to recharge and maintain electric vehicles (aircraft or ground support equipment).[14] Finally, finding civilian airfields capable of supporting military aircraft when flying cross-country will become more challenging and expensive if the DOD lags behind the civilian sector in adopting these technologies. The emergence of these technologies is a net positive, but military aviation needs to get ahead of them before they become unnecessary challenges.

Conclusion

Overall, the U.S. Chamber of Commerce's Global Aerospace Summit was an amazing event and spanned a wide array of topics. Undoubtedly, the military aerospace professionals who spoke at or attended this year likely walked away with different assessments of the future. Voices of the military are key to informed debates about the technological, budgetary, and policy issues surrounding aviation and aerospace. Recognizing this, the U.S. Chamber is seeking to expand the audience of future Global Aerospace Summits and include more representatives from the U.S. military. There should be a similar effort within the Services to ramp up public-private information sharing and collaboration in aviation and aerospace. Robust public-private partnerships and shared strategizing will help the United States soar in these industries, ensure continued U.S. leadership in technology and innovation, and support a dynamic workforce. Otherwise, the U.S. military risks losing its advantage in the highest domains.

Notes

1. Chris Karns, "In Competition for Talent, DOD Needs to Learn, Adapt, or Be Left Behind," *Military Times,* December 10, 2022, and https://www.gao.gov/products/105519; and David Carpenter and Brandon Murrill, "The Buy American Act and Other Federal Procurement Domestic Content Restrictions," *Congressional Research Service,* November 8, 2022, https://crsreports.congress.gov/product/pdf/R/R46748.

2. U.S. Chamber of Commerce, "How Satellites Are Reshaping Modern Conflict," *YouTube* video, 24:44, September 13, 2023, https://www.youtube.com/watch?v=0W3VNM0mMtw&list=PLcNyVG9PAJghA4Pcdl27JPsCl6cL0ZNSz&index=15; and Richard DalBello, Mike Gabor, Austin Link, Ian Thomas, "Navigating the Orbit: Space Situational Awareness and In-Space Servicing and Manufacturing for Space Sustainability," Panel Discussion, 2023 Global Aerospace Summit, Washington, DC, September 13, 2023.

3. U.S. Chamber of Commerce, "Highlights: Global Aerospace Summit 2023," *YouTube* playlist, September 18, 2023, https://youtube.com/playlist?list=PLcNyVG9PAJghA4Pcdl27JPsCl6cL0ZNSz&si=utq611D8bK16GfXp.

4. "How Satellites Are Reshaping Modern Conflict."

5. Kyle Clark, Justin Towles, James Viola, Brian Yutko, "The Future of Air Mobility," Panel Discussion, 2023 Global Aerospace Summit, Washington, DC, September 12, 2023.

6. "Highlights: Global Aerospace Summit 2023."

7. Kevin M. Burke, Kevin Dolliole, David N. Edwards, Jr., "How Infrastructure and Supplemental Funding is Improving Airports," Panel Discussion, 2023 Global Aerospace Summit, Washington, DC, September 12, 2023.

8. "Highlights: Global Aerospace Summit 2023."

9. Ibid.

10. Suzanne P. Clark and Gregory J. Hayes, "*RTX*. Fireside Chat," 2023 Global Aerospace Summit, Washington, DC, September 12, 2023, https://youtu.be/yV3lNjRmndU?si=CFVmRVE8tNuTcMUV.

11. Bob Woods, "How Airlines Plan to Create a New Generation of Pilots Amid Fears of Decade-long Cockpit Crisis," *CNBC,* November 11, 2022, https://www.cnbc.com/2022/11/11/how-airlines-plan-to-create-new-generation-of-pilots-at-time-of-crisis.html.

12. "Highlights: Global Aerospace Summit 2023."

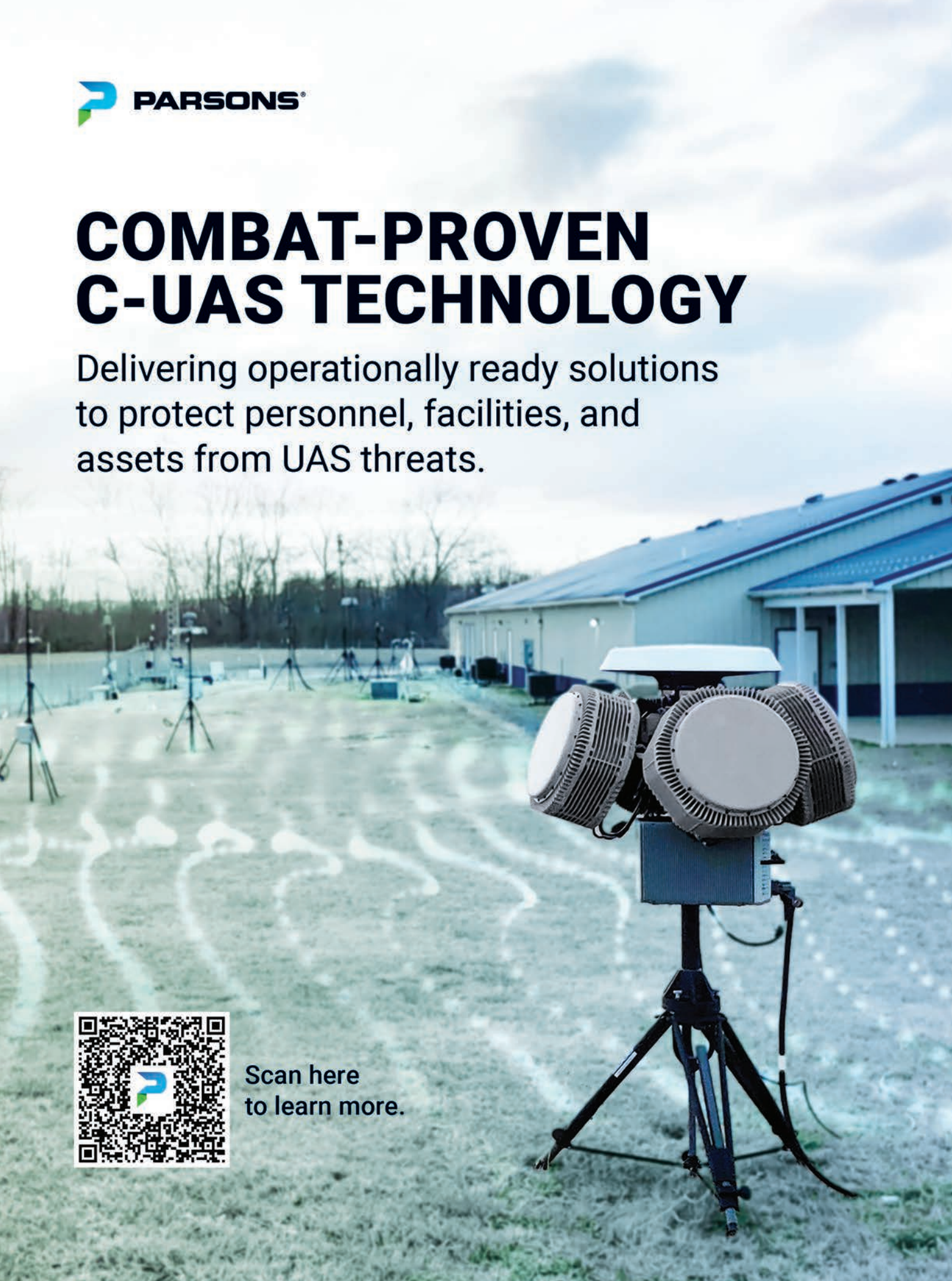
13. Ibid.

14. The Army Applications Laboratory, *"Powering an Electric Vehicle Infrastructure for the U.S. Army,* (Austin: 2021).

PARSONS®

COMBAT-PROVEN C-UAS TECHNOLOGY

Delivering operationally ready solutions to protect personnel, facilities, and assets from UAS threats.



Scan here
to learn more.

Hacking the Minds of Decision Makers

Preparing strategic corporals for future warfare

by Capt Corey A. Ware

In 2017, the Chairman of the Joint Chiefs of Staff established information as a new joint function, which prompted the Marine Corps to adopt it as its own warfighting function.[1] Under this warfighting function, leveraging information through multi-domain operations or all-domain operations dominates the media as persistent buzzwords across the military and private sectors.[2] Many experts strive to understand these concepts; however, the skillful use of information and its powers were demonstrated during the height of the Islamic State of Iraq and Ash-Sham (ISIS) and the Russian aggression in Crimea and Ukraine.[3] The ability to develop unorthodox solutions to complex problems is a hallmark of information planners. Rather than relying solely on history, deployment experience, or wargames where solutions and outcomes are publicly known, information planners encounter problems that cannot be read about in open source due to classification. Placidly, the mindset of an information maneuver professional is no different from any other service member: employing a warfighting approach to exploit an enemy or friendly center of gravity analysis to his or her advantage.[4] As such, creative minds drawing ideas from both fiction and non-fiction can have a significant impact on mission success.[5] In an age of competition, the DOD anticipates operating in a contested information environment. The Marine Corps must send more experienced information maneuver Marines to professional military education and employ them in unit/staff training to equip decision makers and strategic corporals with the ability to plan and incorporate information forces into all levels of war.[6]

>Capt Ware is a Cyberspace Warfare Officer currently assigned as the Senior Cyber Instructor at Marine Detachment Fort Eisenhower. He previously served with Joint Task Force Ares as a Mission Commander and Assistant Operations Officer on a Combat Mission Team for two years, planning and executing offensive cyberspace operations in support of U.S. Cyber Command objectives. Capt Ware has also deployed to Operation Inherent Resolve, where he was both the Joint Task Force Ares Liaison Officer to the Combined Joint Task Force and Cyber Planner in the Information Operations Directorate. During his deployment, Capt Ware collaborated directly with the USCENTCOM Joint Cyber Center, USCENTCOM Cyberspace Operations-Integrated Planning Element, Joint Force Headquarters-Cyber Army, Joint Force Headquarters-Cyber Air Force, and all entities/components planning cyberspace operations within Iraq and Syria. During academic year 2022, Capt Ware was one of two Cyberspace Warfare Officers attending resident Expeditionary Warfare School.

Faculty and students at Marine Corps professional military education (PME) do not possess the requisite knowledge or experience to educate the force on operations in the information environment (OIE).[7] Since the creation of the Marine Corps 17XX information maneuver occupational field (OccFld) in 2022, there has been a limited population of retained Marines and experienced personnel outside of Marine Corps Forces Cyberspace Command (MARFORCYBER), Marine Corps Forces Space Command (MARFORSPACE), and Marine Corps Information Command (MCIC).[8] Even fewer are assigned as instructors or students to formal schools outside of entry-level training.[9] Meanwhile, "numerous state and non-state actors have come to see cyber means as a powerful force multiplier ... [using] malicious cyber to achieve asymmetric advantages, targeting U.S. critical infrastructure and degrading U.S. military superiority ... [threatening] the safety, security, and prosperity of the American people."[10] As the DOD engages in great power competition, MAGTFs "are currently unable to effectively operate in [the information environment] because of a limited number of [OIE] personnel, rudimentary equipment, and a lack of intelligence support. Present deficiencies are addressed through reach back agencies or an arduous request process for specialized support."[11] Furthermore, Marines are not exposed to OIE request processes or planning considerations during PME. Due to a lack of education on OIE, future decision makers and strategic corporals remain unable to make justified decisions involving the employment of information forces or understand how to request effects from an OIE capability.

Training also does not resemble potential OIE effects U.S. forces will encounter against near-peer adversaries.[12] Oftentimes, unit leaders are primarily concerned with completing training vice inducing valid injects or

friction they incessantly face in contested environments with competitors like China, Russia, Iran, and North Korea. These adversaries will deny, degrade, disrupt, destroy, or manipulate information. Potential examples include spoofing a senior officer's account to issue fake or modified orders or even using ransomware to deny funding for logistical movements or supply purchase requests. The most extreme examples of cyber espionage include stealing designs of critical DOD assets since at least 2012 for follow-up exploitation: "the Patriot Advanced Capability-3 air defense system, the F–35 and the F/A–18 fighter aircraft, the P–8A reconnaissance aircraft, the Global Hawk UAV, the Black Hawk helicopter, the Aegis Ballistic Missile Defense System, and the Littoral Combat Ship."[13] Cyberspace attacks could also degrade or destroy command and control assets, as well as the sensing platforms, required to conduct naval gunfire support or fire missions from expeditionary advanced bases on enemy targets ashore.[14] Current unit/staff training places decision makers and strategic corporals at a disadvantage, where trainees lack the ability to develop courses of action incorporating "cyber capabilities to be used in crisis or conflict."[15] Additionally, exponential technological advances and social media have changed the character of war where scrutiny from the media and the court of public opinion will forever compel service members to serve as "the most conspicuous symbol of American foreign policy."[16] Decisions and actions by service members, declared hostile forces, and non-combatants on the battlefield with personal electronic devices can "potentially influence not only the immediate tactical situation but the operational and strategic levels as well."[17] Failure to conduct training with problems service members may face in the information domain will lead to delayed decision cycles. Thus, leaders will remain overwhelmed with trying to devise solutions to complex problems they never experienced or resolved in a training environment.[18]

The rotation of senior and experienced 17XX leaders–staff non-commissioned officers, chief warrant officers, captains, and majors–to PME and key billets throughout the Marine Corps can ameliorate education, training, and the integration of OIE with combatant commander and MAGTF requirements. First, the Marine Corps must increase the 17XX faculty and student population at PME. Gen Berger's *Commandant's Planning Guidance* describes PME as "student-centered learning using a problem-posing methodology

... leaders will remain overwhelmed with trying to devise solutions ...

where our students/trainees are challenged with problems that they tackle as groups in order to learn by doing and also from each other."[19] Lessons learned from a diverse conference group or staff during seminars, lectures, curriculum development, or wargames are intangible, especially when including personnel from the information maneuver OccFld: cyber, psychological operations, electromagnetic spectrum operations, space, and civil affairs. Increasing OIE vignettes in exercise scenarios and non-lethal commentary at PME opens the aperture to a new level of military planning, where future leaders/decision makers can request effects or capabilities that may reside with United States Cyber Command, a joint task force/joint staff, or another governmental organization.[20] By creating a planning environment that normalizes "asking for authorities to use tools in new domains" or other diplomatic, informational, military, economic, financial, intelligence, and law enforcement instruments of power, future planners can maximize the ability to incorporate information fires into all levels of war.[21] Gen Glavy, current Deputy Commandant for Information, challenges 17XX professionals to achieve national military objectives and "educate and empower the rest of Marine Corps [about OIE]."[22] Cultivating OIE enlightenment across the Marine Corps begins with formal education supplemented with training.

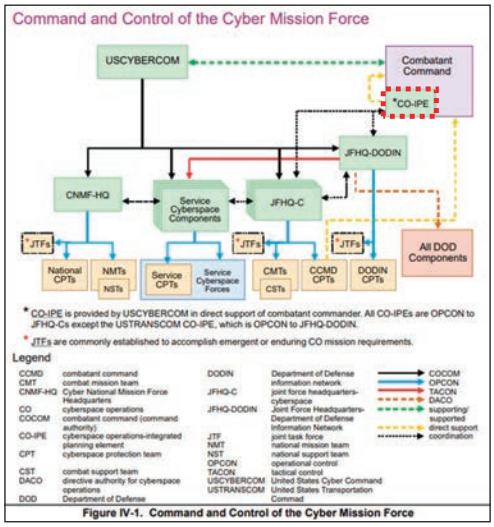


Figure IV-1. Command and Control of the Cyber Mission Force

1702 majors and/or 1710/1720 chief warrant officers as well as 1799 master sergeants/master gunnery sergeants should be embedded in certain or all CCMD COIPEs, who are also co-located with CCMD staffs. ***(Figure provided by the author from Figure IV-1,* JP 3-12 Joint Cyberspace Operations*).***

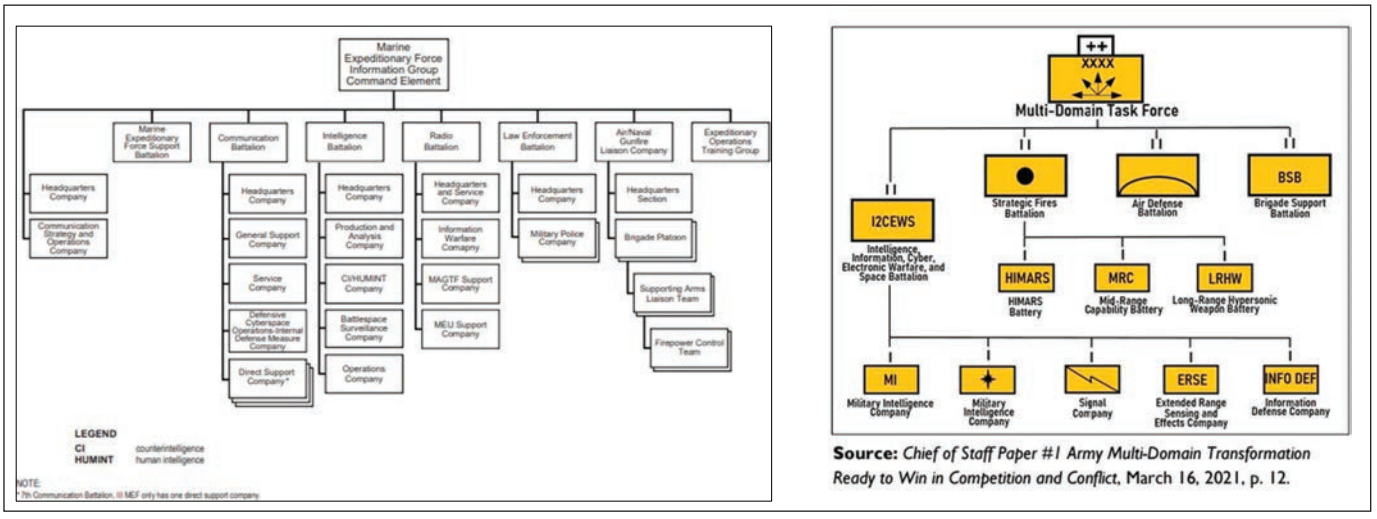
The fusion of command, control, authorities, and responsibilities at MARFORCYBER, MARFORSPACE, and the MCIC presents a multitude of opportunities. In terms of the 17XX cyberspace component of the information maneuver OccFld. assigning subject-matter experts (SMEs) to key billets within the Marine Expeditionary Force Information Groups (MIGs) and Combatant Command Cyberspace Operations-Integrated Planning Elements (CO-IPEs) will assist with training and professionalizing the force about cyberspace operations and OIE writ large. "CO-IPEs are staffed by the [service cyber components]" with personnel who have ideally been on a team or possess relevant operational experience in the cyber mission force "and are co-located with each CCMD [combantant command] for full integration into their staffs."[23] As such, the CO-IPEs provide direct liaison authority/reach back to United States Cyber Command for full spectrum cyberspace planning and execution. The Marine Corps has little to no representation at CCMD CO-IPEs and must create and staff these billets

with experienced 17XX majors/chief warrant officers and senior enlisted personnel to bolster both cyberspace and OIE concepts of support.[24] This buy-in will provide an exponential return on investment, increasing the speed and tempo of cyberspace operations. During real-world planning or wargaming, experienced 17XX cyberspace personnel should compile or generate effects requests to the combatant commander to give them "practice in decision-making against a thinking enemy" because the current generation of commanders are not acclimated to this domain.[25] Furthermore, operational effects in the information environment do not necessarily lead to service members being physically endangered on the battlefield. By conditioning decision makers with non-lethal options, this awareness will boost their confidence in approving the cyberspace concept of operations and other OIE initiatives. The addition of 17XX cyberspace Marines to CCMD CO-IPEs will spawn serendipitous value to a CCMD staff by capitalizing on the Marines' understanding of an amphibious ready group/MEU (Special Operations Capable) employment in the Marine Corps planning process and ability to advance cyberspace opportunities by leveraging an integration between Marine Special Operations Command and MARFORCYBER.[26]

Separately, the MIG is the primary Marine Corps organization tasked with fighting the information environment while simultaneously denying adversaries freedom of action in support of the MAGTF.[27] Key lessons learned from after-action reports and pre-deployment training have shown an appreciation for this new domain based on influence operations synchronized with cyber injects.[28] A recent example of a MIG success includes influence and deception operations during a force-on-force exercise where a battalion commander almost charged a lance corporal for fake, snarky remarks made on social media about the commander and the exercise. The lance corporal's charges were shortly followed by a weather disinformation campaign where weather reports were amplified to create the perception that the weather would end the exercise earlier than expected.[29] If spearfishing emails about the weather were distributed to the entire battalion, then a single click on a malicious hyperlink by just one Marine could potentially compromise the entire battalion's tactical network. The influence operations and cyberspace attack created in the aforementioned vignette could realistically delay decision cycles on actual battlefields rather than just in an exercise. Sending personnel with experience from MARFORCYBER/MARFORSPACE/MCIC, who are also familiar with exercising in virtual environments, will enable the MIGs to design similar exercise networks that can effectively train the operating forces at all echelons of command. "For the Marine Corps to remain competitive as a joint-force contributor, Marines must embrace the information warfighting function" by appointing experienced personnel to key billets to train and advise decision makers and planners: reinforcing the integration of information forces into military operations.[30]

If spearfishing emails about the weather were distributed to the entire battalion, then a single click on a malicious hyperlink by just one Marine could potentially compromise the entire battalion's tactical network.

A counterargument claims decisive actions against a near-peer adversary will involve physical maneuver using expeditionary advanced based opera-



Source: *Chief of Staff Paper #1 Army Multi-Domain Transformation Ready to Win in Competition and Conflict*, March 16, 2021, p. 12.

The Marine Corps and Army possess similarities between the MIGs and MDTFs, prompting collaborative efforts. *(Figures provided by the author from Figure 4-1,* **MCRP 1-10.1** *Organization of the United States Marine Corps [left] and The Army's MDTF Congressional Research Service report dated 16 March 2023 [right]).*

LtGen Glavy, CG, U.S. Marine Forces Cyberspace Command, speaks with Marines during MAGTF Warfighting Exercise 2–23. *(Photo by LCpl Pedro Arroyo Jr.)*

Transitioning from a generation of counterinsurgency operations, Gen Smith has made it clear the Marine Corps must "partner and integrate with the Navy at every level possible to provide the joint force with sea based expeditionary forces" ...

Then BGen Bill Seely, Task Force Iraq commander, visited the Ministry of Peshmerga in Erbil, Iraq, 2019. *(Photo by Sgt 1st Class Gary Witte.)*

tions; the Marine Corps does not need to focus on the information warfighting function during training to achieve success. Although service members will need to operate "from the thin air and high altitudes of the mountains, to the sweltering heat of triple canopy jungles," it blatantly disregards a critical requirement: placement and access inside an enemy's weapon engagement zone. This will require the synchronization of influence operations, deception of the adversary's sensors and common operational picture, and electronic warfare to enable effective lethal fire and maneuver.[31] Transitioning from a generation of counterinsurgency operations, Gen Smith has made it clear the Marine Corps must "partner and integrate with the Navy at every level possible to provide the joint force with sea based expeditionary forces" by embracing naval integration and immersing the FMF into understanding the Navy's composite warfare concept.[32] Marines on the keyboard or developing OIE concepts in a sensitive compartmented information facility will not be crucial to mission success on the battlefield; the priority of efforts should address only the MEUs and amphibious exercises to meet the commandant's intent. PME and unit/staff training "must be focused on winning in combat in the most challenging conditions and operating environments."[33] Therefore, incorporating OIE into education and training should be secondary.

Irrevocably, operations in the information environment will continue to dominate current and future warfare. In planning rooms of the operating forces and behind closed doors at the Pentagon, it is paramount that senior decision makers and strategic corporals possess the right education and training to succeed. In a future operating environment, it is no longer about "the smartest person in the room [or the most senior] ... the smartest guy or gal in the room is the room."[34] Victory in future warfare will demand Joint Force and whole of government alliances and partnerships, with credible suggestions derived from the lowest levels. By integrating experienced 17XX information maneuver professionals into PME—as

students and instructors—and placing them in critical billets, the Marine Corps and DOD will ensure the right planners are in the room to drive operational requirements and objectives. This simple hack will allow us to train each other and develop options for decision makers across the range of military operations, using the competition continuum as a reference point.[35]

Notes

1. Gen Robert B. Neller, *MCBul5400, Establishment of Information as the Seventh Marine Corps Warfighting Function*, (Washington, DC: February 2019).

2. AFCEA International and the U.S. Naval Institute, "02 14 23 USMC Theater Multi-Domain Operations and Joint/Naval Expeditionary Killwebs," *YouTube*, 20:18, February 20, 2023, https://www.youtube.com/watch?v=Xb_HdqJaBKA&t=2041s.

3. Corey Klonowski, "The Seventh Warfighting Function," *Marine Corps Gazette*, September 2021, https://www.mca-marines.org/wp-content/uploads/The-Seventh-Warfighting-Function.pdf.

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

5. Peter W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media* (Boston: Eamon Dolan/Houghton Mifflin Harcourt, 2018).

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

7. Information available at https://www2.manpower.usmc.mil/ncp/mosDistri.

8. Matthew G. Glavy, *MARADMIN 102/22 Establishment of the Information Maneuver 1700 Occupational Field* (Washington, DC: 2022).

9. Information available at https://www2.manpower.usmc.mil/ncp/mosDistri.

10. Department of Defense, *Summary 2023 Cyber Strategy of The Department of Defense*, (Washington, DC: 2023).

11. Austin Duncan, "On Cyber," *Marine Corps Gazette,* April 2018.

12. Commanding General, Marine Air Ground Task Force Training Command, *Final Exercise Report for MAGTF Warfighting Exercise 2-23*; Commanding Officer, Marine Corps Information Operations Center, *After Action Report Information Warfighter Exercises for Calender Year 2023 (IWX 23-1, 23-2, 23-3, 24-1)*; Commanding Officer, 2nd Battalion, 7th Marines, *V27 After-Action Report for Integrated Training Exercise (ITX) 5-23 From July to 31 August 2023* (Quantico: Marine Corps Center for Lessons Learned, 2023).

13. U.S.-China Economic and Security Review Commission, *2014 Report to Congress of the U.S.-China Economic and Security Review Commission*, (Washington, DC: 2014).

14. Commanding Officer, 15th Marine Expeditionary Unit, *Combined After Action Report for Amphibious Ready Group and Marine Expeditionary Unit Exercise and Composite Training Unit Exercise*, (Quantico: Marine Corps Center for Lessons Learned, 2021).

15. Lloyd J. Austin III, *2022 National Defense Strategy of The United States of America*, (Washington, DC: 2022).

16. Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War," *Marines Magazine*, January 1999.

17. Ibid.

18. *Combined AAR for ARG and MEU Exercise and Composite Training Unit Exercise*; and Commanding Officer, Marine Corps Information Operations Center, *Marine Corps Information Operations Center (MCIOC) After Action Report for Exercise Trident Juncture-18 (TRJE-18)*, (Quantico: Marine Corps Center for Lessons Learned, 2019).

19. *38th Commandant's Planning Guidance.*

20. Air Land Sea Application Center, *Multi-Service Tactics, Techniques, and Procedures for Joint Application of Firepower*, *JFIRE/ATP 3-09.32/MCRP 3-31.6/NTTP 3-09.2/AFTTP 3-2.6*, (Washington, DC: Air Land Sea Application Center, 2019).

21. Headquarters Marine Corps, *MCDP 1-4, Competing*, (Washington, DC: December 2020).

22. MARFORCYBER, "Leading Cyber Marines with MajGen Matthew G. Glavy," *YouTube*, 14:32, January 20, 2021, https://www.youtube.com/watch?v=jY730Jwmo18.

23. Joint Chiefs of Staff, *Joint Cyberspace Operations*, Joint Publication 3-12, (Washington, DC: 2022).

24. Information available at https://www2.manpower.usmc.mil/ncp/rank Mos;mos=1702;mosType=P.

25. *38th Commandant's Planning Guidance.*

26. Tyler Bahn, "Advancing Cyberspace Operations: Opportunities to Leverage MARSOC and MARFORCYBER," *Marine Corps Gazette*, January 2022, https://mca-marines.org/wp-content/uploads/Advancing-Cyberspace-Operations.pdf.

27. Information available at https://www.iiimef.marines.mil/Units/III-MIG.

28. *Combined AAR for ARG and MEU Exercise and Composite Training Unit Exercise*; and *After Action Report for Exercise Trident Juncture 18*.

29. Brian Russell, "The Five OIE Truths: What it Takes to be Successful in the Information Environment," *Marine Corps Gazette,* April 2021, https://mca-marines.org/wp-content/uploads/The-Five-OIE-Truths.pdf.

30. *MCDP 8, Information*.

31. *38th Commandant's Planning Guidance.*

32. Eric M. Smith, "Guidance to the Force," White Letter 1-23, Assistant Commandant of the Marine Corps (Washington, DC: 1 August 2023).

33. *38th Commandant's Planning Guidance.*

34. MARFORCYBER, "MARFORCYBER Panel at Minority Innovation Weekend (2020 National Cybersecurity Awareness Month)," *YouTube*, 1:02:01, January 12, 2021, https://www.youtube.com/watch?v=v2LKPCOvxS4&t=3996s.

35. *MCDP 1, Competing.*

ASTRONICS
TEST SYSTEMS

Elevated radio maintenance for operational readiness

CTS-6010
Tester of choice
for the US Marines
HHRTS program

ATS-3100 RTS
Tester of choice
for the US Army
TS-4549/T program

When it comes to preparation, your fleet comes first. The ATS-3100 RTS (benchtop) and the CTS-6010 (portable/handheld) radio test solutions from Astronics help maximize your operational readiness by ensuring your radios perform when needed. With support for legacy, modern, and future technology, our solutions are the ideal replacement solutions for aging and unsupportable test equipment.

Contact us today to get started.

TEST SOLUTIONS

LEARN MORE

Building All-Domain Communicators

An MOS structure for the communicator of the future

by Maj Adrian Felder, Capts Ed Frasier, Philip King, Ben Williams & MGySgt Ben Price

To stay relevant and adaptable in the modern tactical landscape, the Marine Corps' 06XX Communications field must undergo a transformation. Rapid advancements in technology and the expansion of the information environment have rendered our current MOS structure—rooted in post-Cold War communications concepts—inadequate for meeting the evolving needs of commanders. The future 06XX field must prioritize cross-disciplinary foundational concepts and foster a culture that promotes knowledge sharing, continuous learning, and skill development at all levels.

>Maj Felder serves with the 3d MarDiv Communications Company.

>>Capt Frasier serves at The Basic School.

>>>Capt King serves at the 7th Communication Battalion.

>>>>Capt Williams serves with MAG 12.

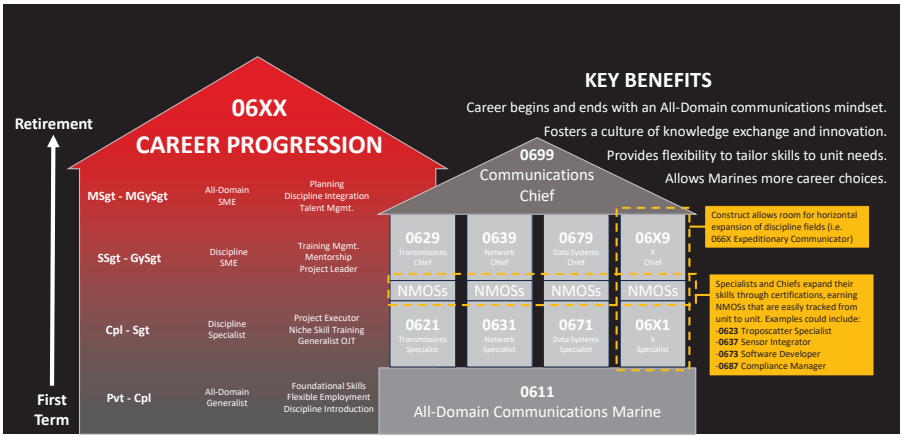
>>>>>MGySgt Price serves with the 2d MarDiv Communications Company.

Future Community Requirements

There are three elements that differentiate the future 06XX community from the status quo: communicators must enable the Marine Corps Enterprise Network, be employable in cross-functional communications teams as small as two Marines, and be able to rapidly adapt to emergent systems and networks.

While Marine Corps Headquarters information, command, control, communications, and computers has identified that the warfighting network of the future will be the Marine Corps Enterprise Network, our MOS structure has not adapted to this reality.[1] Marine Corps Cyber Operations Group and the network battalions now provide services previously maintained at the tactical edge, changing the skill requirements for communications Marines. Future communicators must understand the breadth of this network and be trained to support it from various echelons. Even transmissions Marines—who previously had little to do with internet protocol employment—now are intertwined with it. Future Marine Corps Enterprise Network enablers must have a broad foundation of knowledge to enable a vast collection of command and control services across the enterprise network.

Commanders have recently communicated the need for communicators who possess a broader range of skills and are able to maneuver in the information environment as small teams. This requirement has resulted in the development of the Expeditionary Communicator Course by the Communications Training Battalion.[2] Currently in experimentation, this course has been successful in producing all-domain communications NCOs able to operate independently at not just in infantry units but in other FMF units where small nodes are critical. However, with the current construct, the number of expeditionary communicators in any given unit will be limited to a handful. The future MOS structure must take the lessons learned from Expeditionary Communicator Course and scale



All-Domain Communicator Concept diagram depicts proposed all-domain communicator career progression and skillsets. *(Diagram provided by author.)*

it across the 06XX forces to provide increased communications flexibility and maneuver to all FMF commanders.

Commanders also have more ability than ever before to procure and integrate non-program of record communications capabilities at lower echelons, resulting in communicators operating a far wider range of systems—more than can be taught in a single course. The introduction of commercial off-the-shelf systems like MPU-5s, PACSTAR suites, and Kymeta terminals—all internet protocol-based—means that future communicators must be trained to rapidly integrate new technologies that they may have no formal instruction on. To do this, formal training must focus on underlying concepts to enable technical decision making, not the operation of specific systems.

MCWS-X Night. Marines with 3d MarDiv Communications Company establish a Marine Corps Wideband Satellite Expeditionary terminal as part of an expeditionary communications node. ***(Photo provided by author.)***

A New Structure

To meet these requirements, we propose changing the career path for 06XX enlisted Marines by developing all-domain communications generalists who then progress to become discipline specialists after their first term. The entry-level 06XX Marine changes from discipline-specific (i.e. 0621s, 0631s, etc.) to an 0611 all-domain communications Marine. 0611s are trained in foundational communications knowledge, from radio frequency propagation to internet protocol subnetting, providing a knowledge base to be leveraged in various positions. 0611s will graduate from entry-level training able to be positioned in any basic communications billet. From there they will receive on-the-job training from specialists (NCOs) and chiefs (SNCOs) specific to a unit's requirements.

The second tier of this structure is the discipline-specific specialists we are accustomed to—though the disciplines themselves may change as communications evolve. Transitioning at their first re-enlistment, retained 0611s will compete for specialist boat spaces like 0627 satellite operator or 0661 expeditionary communicator. MOS selection will be based on the experiences at their first unit as well as personal preference. As NCOs, these second-term communicators will be required to attend the respective supervisor's course for their discipline, which will serve as the MOS granting school. Through this training, specialists will acquire the knowledge to put them on the path to becoming experts while retaining the all-domain communications mentality learned as an 0611.

After NCO, specialists advance to their respective chief MOS. Completing the chief's course through a blend of virtual and in-person MCCES instruction, these SNCOs advance to be not only a subject-matter expert in their discipline but also educated in communications integration and how to manage and conduct effective on-the-job training within their units. The training role is critical within the new paradigm due to the chiefs' responsibility to facilitate knowledge transfer between the NCO specialists and the newly minted 0611s in alignment with a unit's mission. By placing technical knowledge transfer at the forefront of chiefs' responsibility, we ensure that training and technological evolution remain at the forefront of the 06XX community.

The top tier of the enlisted career path does not change. Upon reaching E-8, discipline chiefs transition to be 0699 communications chiefs. With all communicators beginning their careers as generalists and with a continued emphasis on discipline integration through the NCO and SNCO ranks, this transition will become more streamlined. Through the E-1 to E-9 progression, enlisted communicators now begin and end their careers maneuvering across the entire communications domain.

Community Benefits

This structure provides organizational, operational, and cultural benefits. Organizationally, the structure emphasizes retention of quality 0611 Marines as they transition to specialists due to the increase in career agency provided to the individual Marine, aligning with *Talent Management 2030*'s direction to both leverage Marines' pre-existing talents and increase lateral move flexibility. This agency begins at a Marine's arrival at her first unit with her ability to explore various communications disciplines and continues at her first re-enlistment with the selection of a specialist MOS tailored to her experiences and knowledge. Providing this autonomy to the Marine will be done with no negative impacts on Service requirements, utilizing first-term boat spaces to ensure that MOS staffing is met.

Operationally, the flexibility enabled within the FMF is critical to communicators' ability to adapt to future missions and technologies. Through the introduction of the 0611, the 06XX adopts a mentality of *any communicator,*

any system, similar to the *any Marine, any weapon* arms room concept introduced in *Infantry Battalion Experiment 2030*. Units decide what systems—what "weapons—they need their communicators employing and are able to train first-term Marines on mission-specific equipment. With support from the discipline specialists and chiefs, all-domain communicators will enable more efficient troop-to-task organization and the deployment of smaller communications elements.

Our structure creates a culture of knowledge transfer and training to ensure the long-term sustainment of the community as a learning organization. The combination of all-domain generals and discipline specialists, chiefs, and trainers and their interdependency on one another breaks down the current walls between our siloed MOSs. It is the specialist's job to provide training for the 0611s he leads and the chief's job to oversee this training and ensure the 0611s are employed where and how the unit needs it. The addition of necessary MOSs for skills that have historically been taught but not tracked emphasizes the fact that training and education are continuous. Marines begin and retire from their careers as all-domain communicators.

Challenges

The most significant challenge that the all-domain communicator concept faces is defining and developing the 0611 MOS. Marine Corps Communication-Electronics School must distill the key concepts of current entry-level courses into an all-domain communicator course of similar length. It can do this by focusing the 0611 periods of instruction on critical communications functions (i.e. communications security practices and systematic troubleshooting) and theory (i.e. radio frequency propagation and internet protocol routing and switching) while removing system-specific training. The end state is that entry-level 0611s have enough knowledge to make them successful when they reach their first unit while not delaying the current training timeline.

Changing the community's culture regarding follow-on technical training and education must also be addressed. Without an emphasis on knowledge transfer and continuous learning, this MOS structure will likely fail. To ensure 0611s, specialists, and chiefs maintain and adapt their skills within the technological operating environment, FMF units must bear some responsibility for technical training facilitation. This will require allocating manpower to the problem, which is why chiefs will take an active role in it. SNCOs must drive the training plans for their Marines, coordinating on-the-job training as necessary while also leveraging external organizations like communications training centers and Marine Corps Tactical Systems Support Activity. Units should want to send their Marines to training. It is short-term pain that reaps long-term benefits.

Driving the Transformation

Transforming our current stovepiped MOS structure into one that embraces the all-domain communication concept is a challenging endeavor that will not be accomplished quickly or effortlessly. It requires a collaborative effort between all stakeholders including Manpower and Reserve Affairs, the occupational field manager, Marine Corps Communication-Electronics School, monitors, and FMF units. However, by steering the communications community in this direction, we ensure we will possess the necessary training and personnel to effectively deliver communications in future operating environments, whatever they may look like.

MCWS-X Day. Marines with 3d MarDiv Communications Company establish a Marine Corps Wideband Satellite Expeditionary terminal as part of an expeditionary communications node. ***(Photo provided by author.)***

Notes

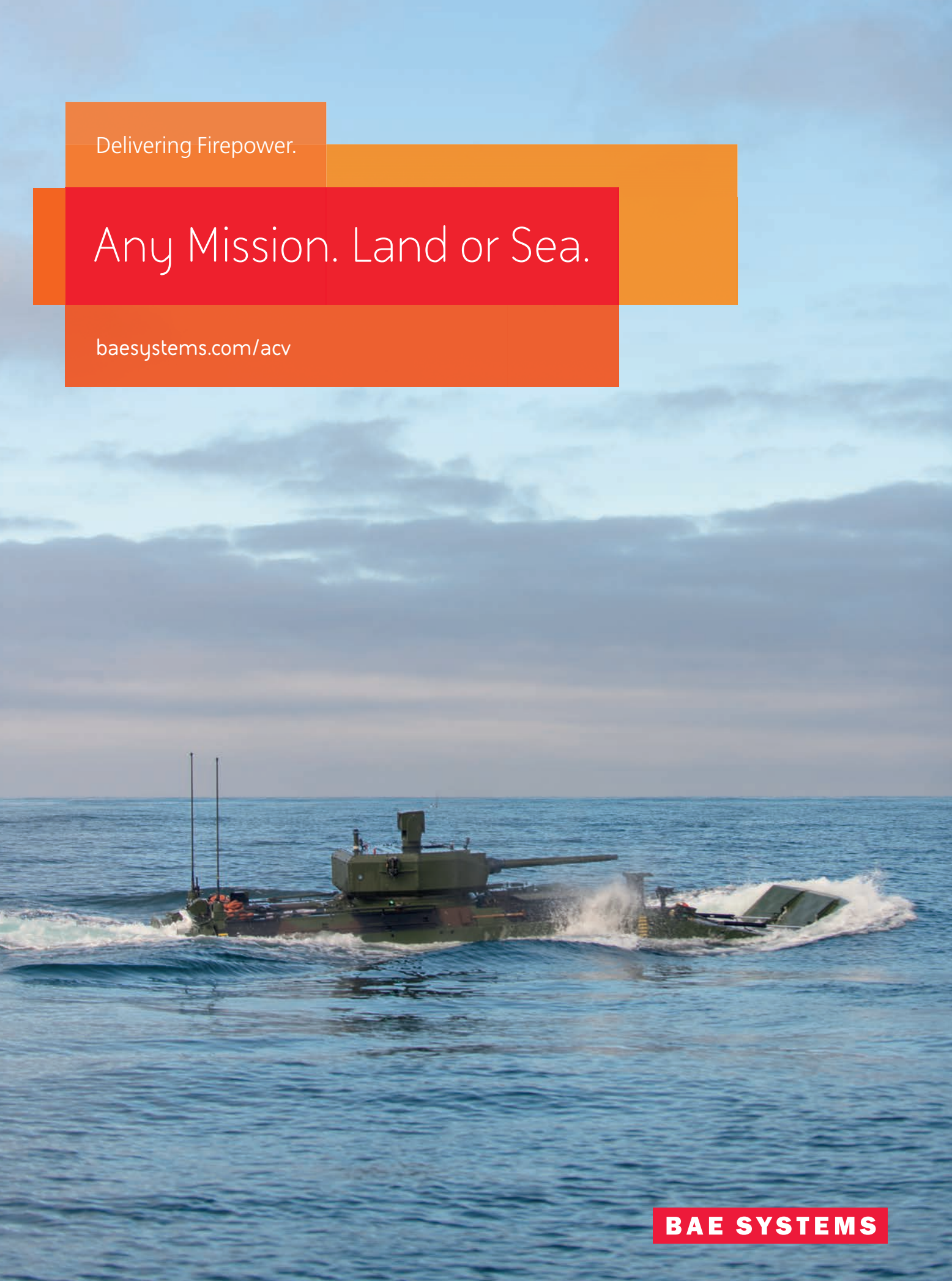
1. Information Division, Capabilities Development Directorate, Combat Development & Integration, *Marine Corps Enterprise Network 2030 Concept of Employment (COE)*, (Quantico: 2023).

2. Marine Corps Communications-Electronics School, *Communicator of the Future Initiative Overview Version 7*, (Twentynine Palms: 2021); and Gidget Fuentes, "Pilot Course Aims to Build Marines' Skills as Communicators for the Future Fight," *US Naval Institute News*, February 28, 2023, https://news.usni.org/2023/02/28/pilot-course-aims-to-build-marines-skills-as-communicators-for-the-future-fight.

Delivering Firepower.

Any Mission. Land or Sea.

baesystems.com/acv



BAE SYSTEMS

Managing CMMC Status Validation for COTS Equipment in Gray Space Acquisitions

Strategic approaches to CMMC compliance in gray-space technology acquisitions

by Maj Lawrance Andrus Jr.

The DOD encounters unique obstacles when securing its systems and networks in an evolving landscape. The acquisition and management of commercial-off-the-shelf (COTS) items within the gray cyberspace realm present challenges. These difficulties arise from the differences in vulnerability management between blue cyberspace devices and the "green gear" devices that operate within the gray cyberspace realm. Acquiring DOD blue space devices may only sometimes be practical as DOD priorities differ in this context. As a result, the convenience and functionality gained through gray-space procurements often come at the expense of security, introducing risks to operations. Effectively addressing this issue requires management of Cybersecurity Maturity Model Certification (CMMC) status validation for COTS equipment obtained in gray space to safeguard confidentiality, integrity, and availability.

>See bio on page 36.

The Challenge of Acquiring Devices in Gray Space

The gray cyberspace realm presents an environment where distinguishing between adversary activities becomes challenging. Within this arena, the DOD confronts the task of procuring green devices primarily comprising COTS items while ensuring their cybersecurity meets standards. In contrast to blue cyberspace, where the DOD can control device specifications and security standards, the emphasis on cyber hardening may be lower in gray-space acquisitions. Regarding gray-space investments, it is often not practical for the DOD to purchase devices to those found in blue space. The DOD's obligations and priorities differ between these two realms. For instance, while a Samsung S20 device may undergo cyber hardening in blue cyberspace, a device obtained through gray-cyberspace channels, like Samsung S20s obtained via Persistent Systems Inc., may not receive the same priority level.

The Trade-Off Between Convenience and Security

In the pursuit of convenience and functionality, the DOD has adopted COTS equipment procured in gray space. Undoubtedly, this has improved efficiency and flexibility in operations and introduced security risks requiring attention. Introducing COTS equipment into the blue-space environment has expanded the attack surface and increased vulnerability to cyber threats. These devices might have undergone different security evaluations than their counterparts in blue space. Consequently, they can become targets for adversaries seeking to exploit these vulnerabilities. Therefore, while gaining convenience and functionality from procurement practices, the DOD must acknowledge this security trade-off and take measures to communicate and mitigate these risks.

The Issue: Managing COTS Equipment in Gray Space

One of the challenges faced by the DOD is effectively managing COTS equipment obtained in gray space to ensure confidentiality, integrity, and availability. This problem has implications as compromised devices could jeopardize military operations, sensitive information, and national security. Possible solution: collaborating with external vendors. A solution to address the challenges associated with managing COTS equipment in gray space is to collaborate with third-party vendors specializing in cybersecurity and CMMC status validation. These vendors can oversee DOD equipment procurement, mainly focusing on acquisitions within gray space. Relying solely on internal

DOD processes to tackle this issue has limitations, mainly due to procedures that often need to be revised. Engaging a third-party vendor becomes an option to expedite the resolution and ensure that COTS equipment in gray space meets cybersecurity standards.

Advantages of Involving Third-Party Vendors

1. *Expertise and Efficiency*: Third-party vendors possess knowledge in cybersecurity and CMMC compliance. They can efficiently validate the security posture of COTS equipment while ensuring it aligns with required standards. Their agility and focus on cybersecurity contribute to expediting the validation process.
2. *Enhanced Collaboration*: By collaborating with vendors with expertise in this domain, there is an opportunity for cooperation between various stakeholders involved in managing COTS equipment within gray space. This collaborative approach fosters improved communication channels and shared expertise for outcomes.
3. *Independent Validation*: Third-party vendors offer a perspective on COTS equipment, ensuring that biases or limitations do not influence DOD assessments. This independent validation adds credibility to the verification of CMMC status.
4. *Streamlined Processes*: The DOD's bureaucratic procedures can be slow and burdensome. Involving third-party vendors helps expedite these processes, ensuring the validation and deployment of COTS equipment.
5. *Efficient Resource Utilization*: The DOD can optimize its resources by leveraging third-party vendors. Using manpower and expertise to validate CMMC status, the DOD can focus on its primary missions while relying on specialized vendors for this essential task.
6. *Scalability*: Third-party vendors can scale their services based on the evolving needs of the DOD. As technology advances, the DOD can expand its validation efforts with support from these vendors.

Challenges and Considerations

While engaging third-party vendors presents a solution for managing COTS equipment in gray space, some factors need careful consideration:

1. *Vendor Selection*: Choosing vendors with a proven track record in cybersecurity and CMMC validation is crucial for success.
2. *Data Security*: Handling sensitive military data necessitates security measures. Vendors need to demonstrate their capability in safeguarding information.
3. *Cost Benefit Analysis*: Considering the costs of involving third-party vendors compared to the benefits is crucial. Even though it may result in expenses, the enhanced security and reduced risk of compromise can justify the investment.
4. *Regulatory Compliance*: Vendors must comply with regulations and standards that govern cybersecurity, data protection, and CMMC validation.
5. *Integration with DOD Processes*: The collaboration between the DOD and third-party vendors should be seamless. It is crucial to have communication and integration with existing DOD processes.

Conclusion

Managing vulnerabilities in COTS equipment obtained in gray space presents a complex challenge for the DOD. While convenience and functionality are factors, they should not compromise security. Recognizing the importance of validating vendors' CMMC status is a step toward addressing this issue. Engaging third-party vendors who excel in cybersecurity and CMMC validation can expedite the process while ensuring that COTS equipment meets security standards. These vendors bring expertise, independence, and efficiency, reducing delays and optimizing DOD resources. In a world that is becoming more interconnected and filled with cyber threats, the DOD must prioritize the security of COTS equipment in gray-space acquisitions. This goes beyond compliance; it is an aspect of national security. The DOD can strengthen its cybersecurity measures by forming partnerships with third-party vendors and provide enhanced protection for its personnel and assets in gray cyberspace.

USMC

Relying solely on internal DOD processes to tackle this issue has limitations, mainly due to procedures that often need to be revised.

Adding Focus to Digital Frameworks

A strategic move

by Maj Lawrance Andrus Jr.

While the Marine Corps has always embraced advancements, the fast-paced digital transformation calls for a shift toward software-centric solutions rather than just relying on hardware. This transition is not only driven by technology but also strategically important. By integrating artificial intelligence (AI) and blockchain technologies into domains such as predictive maintenance, intelligence analysis, cybersecurity, and coalition operations, the Marine Corps can significantly transform its operations.

The transition towards digital frameworks is a trend and a strategic imperative. As modern battlefields become increasingly complex, quick, data-driven decision making has become paramount. AI and blockchain technologies provide the Marine Corps with the necessary tools to adapt and excel in this new era of warfare.

AI

Anticipatory Maintenance

Using AI algorithms makes it possible to analyze equipment data and anticipate when a piece of machinery is likely to experience failure. This proactive approach to maintenance allows for repairs, minimizing downtime, and enhances operational efficiency. The advantages go beyond cost-saving measures; they directly impact the success of missions.

Furthermore, the application of AI in maintenance can be extended to various types of equipment ranging from vehicles to weapons systems. This adaptability makes AI an invaluable asset in ensuring the readiness of the Marine Corps.

>See bio on page 36.

Intelligence Analysis

Through its ability to process large amounts of data, AI can uncover patterns or threats that might elude human analysts. This capability significantly enhances the speed and accuracy of intelligence gathering, thereby improving decision-making processes.

Moreover, AI has the potential to aid in filtering out noise from vast amounts of data, allowing for the discovery of valuable insights. This becomes particularly advantageous in warfare scenarios where adversaries employ unconventional tactics and blend into civilian populations.

Autonomous Systems

AI can guide drones and other unmanned systems to carry out tasks such as reconnaissance or supply operations. These autonomous systems minimize the risks faced by personnel and can operate effectively in otherwise inaccessible environments.

Additionally, deploying these systems in coordinated groups allows tackling intricate missions that pose challenges for individual units. This collective intelligence displayed through swarm technology proves valuable during reconnaissance missions, search and rescue efforts, and even combat situations.

Cybersecurity

AI algorithms can actively monitor network behavior and swiftly identify abnormal patterns indicative of cyberattacks—often faster than traditional cybersecurity measures. In an increasingly prevalent era of cyber warfare, the Marine Corps must stay ahead with robust cybersecurity measures.

Furthermore, AI can be utilized to safeguard communication channels, ensuring the confidentiality and integrity of information. This is especially crucial in environments where secure communication is paramount.

Combat Simulation and Training

AI can simulate combat scenarios in realtime, enabling more effective and diverse training sessions. Traditional training approaches often rely on set scenarios that may not adequately prepare Marines for the unpredictability of real-world operations.

Moreover, these simulations can be customized based on unit performance, providing targeted training that addresses specific weaknesses. This level of customization was previously out of reach with traditional training methods and represents a significant advancement in combat readiness.

Decision Support

AI can analyze variables in complex situations and provide commanders with recommendations during decision-making processes. In the heat of battle, commanders are faced with making decisions that could have far-reaching consequences. AI can assist by analyzing large volumes of data to provide practical insights.

Additionally, the use of AI in decision support is not limited to combat situations. It can also be applied to administrative tasks, allocating human resources toward more intricate responsibilities that require emotional intelligence and nuanced comprehension.

Blockchain

Ensuring Security in Supply Chains

Blockchain has the potential to create records detailing the origin, handling, and current location of each piece of equipment within a supply chain. This reduces the risk of fraud or tampering. In operations, maintaining the integrity of the supply chain is critical because any compromise can lead to mission failure and put lives at stake.

Furthermore, the transparency provided by blockchain can significantly enhance supply-chain efficiency. It enables realtime tracking of assets, facilitating inventory management and anticipating requirements.

Enhanced Communication Security

Blockchain cryptographic features can make intercepting or tampering with communications complex. In an evolving landscape of information warfare, it is crucial to emphasize the importance of secure communication channels.

Moreover, blockchain can establish networks that are less susceptible to attacks. This becomes particularly valuable when centralized communication hubs are impractical or face the risk of compromise.

Verification of Identity

Blockchain presents a tamper-proof method for managing digital identities, significantly reducing the risks of identity theft or impersonation. In operations, ensuring accurate identification is paramount for maintaining security.

Additionally, blockchain-based identity verification can be employed in coalition operations to guarantee that only authorized personnel can access sensitive information. This can substantially enhance the security and effectiveness of operations.

Data Integrity and Accountability

Blockchain technology allows the creation of an immutable and secure record encompassing various data types, such as personnel records and mission reports. Ensuring the integrity of data holds importance for both operational success and accountability.

In operations, maintaining the integrity of the supply chain is critical ...

Moreover, this technology establishes a system where every action is meticulously documented and subject to audit, thereby introducing accountability in military operations.

Conclusion

Integrating AI and Blockchain technologies offers numerous advantages to the Marine Corps. Shifting from hardware-based systems to digital frameworks represents both a technological transition and a strategic imperative.

Embracing these technologies can substantially enhance efficiency, security measures, and decision-making capabilities. The Marine Corps stands to gain significantly from this transition, positioning itself as a leader in modern warfare.

Refocusing Cyberspace Technology

Optimizing for the conflict phase of war

by LtCol Arun Shankar

The emergence of China and Russia as peer threats has illuminated a new vector for the Marine Corps. The result is *Force Design 2030* and a heavy focus on the competition phase of war. Cyberspace technological advances have followed suit. Immediate commercial-off-the-shelf solutions are now preferred over legacy acquisition. Offensive cyber operations emerged as a legitimate warfighting capability in the cyberspace domain. Moreover, government civilians in the information technology (IT) workforce and acquisition fields remain a significant part of this comprehensive effort.

Even so, many of these solutions are presently optimized for *competition* but not *conflict*. A dependence on commercial solutions and contractor support has drawbacks in deployed, kinetic environments during conflict. Additionally, offensive cyber operations are not yet tuned to readily support tactical conflict. Moreover, the government civilian information technology and acquisition workforces are not adequately incentivized to innovate at the tempo of conflict, resulting in an unnecessary, parallel dependence on outside vendors. The following sections defend these concerns and suggest ways to address them.

>LtCol Shankar is the Deputy Current Operations Officer at USSPACECOM after recently serving as the Commanding Officer, Communication Training Battalion and AC/S G-6, 1st MarDiv. He has also served a combined 28 months in Operations Iraqi Freedom and Enduring Freedom as a counter-IED Analyst, COIN Assessments Analyst, and Communications Officer, and holds a PhD in Operations Analysis from George Mason University.

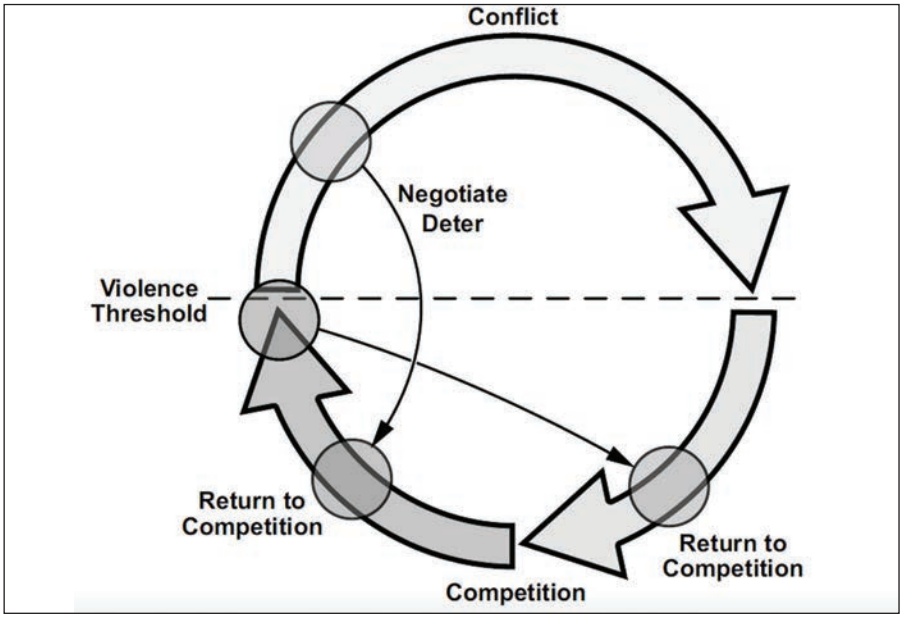


Figure 1. Conflict vs. Competition (*MCDP 1-4*). *(Source:* MCDP 1-4 Competing.*)*

Conflict vs. Competition

We describe the conflict phase of war as kinetic warfare between peer adversaries. During this phase, uniformed service members engage in their traditional, unique combat roles, primarily in forward-deployed locations. Clearly, conflict should be avoided when possible because the aggregate losses could be inconceivable. Accordingly, America's adversaries are convinced that the costs of warfare outweigh the benefits of peace. We maintain this equilibrium by preparing our Marines for conflict, ensuring *every* Marine is trained and deployable with the finest warfighting capabilities.

Competition, a more active form of deterrence, is the constant state of power balance between nations. This phase of warfare has led to the growth of the information domain and the gray zone, where adversarial nations seek to make incremental gains against one another without provoking outright conflict. Consequently, cyber and influence capabilities are now engaged in daily, real-world operations. *Force Design 203*0 energized the Marine Corps' role in competition, emphasizing the purpose of gray-zone activity and stand-

in forces. After years of land battles in the desert, this imperative direction has oriented the total force magnificently. Certainly, competition is the universally preferred position on the warfighting continuum (Figure 1 on previous page), but we only remain here by deterring conflict. However, to do so, cyberspace technology must convincingly support this premise.

Challenges

Commercial solutions

Industrial-age acquisition processes with multi-year development timelines are no longer viable ways to implement cyberspace technology for conflict. By the time these solutions are realized, they are obsolete. Costly requirements analysis and spiral development processes led by the military are no longer necessary. Instead, commercial vendors perform these tasks for us and provide instant, off-the-shelf solutions. The cost savings from traditional acquisition are often returned in software updates, bulk spares, and hotline support, making these solutions extremely practical. In response, every MEF has developed parallel operations and maintenance budgets to purchase such technology from companies like Google, ViaSat, Microsoft, and Cisco. Instant hardware and software are delivered to the FMF, while the maintenance and complexity of these systems are retained in commercial data clouds or warranty repair depots. Resilient satellite links and fiber optic transport validate this course of action during Service-level exercises. The end state is fast and reliable capabilities maintained mainly by vendors, easing the burden on uniformed service members and greatly aiding our efforts during competition.

However, a closer analysis of this circumstance yields concerns about effectiveness during conflict. First, excessive dependence on vendor support during high-intensity battles may be unrealistic. I have several personal examples of vendors failing to adequately support equipment fielding and command and control systems in Afghanistan and Iraq. Though some of this can likely be blamed on shotty contracting, I argue the vendors were generally averse to overseas duties after their equipment was sold and distributed to the military. To further complicate matters, proprietary restrictions often prevented Marines from adequately configuring and repairing specific systems and equipment, rendering them useless when they were most needed.

Realistically, this should not be a surprising conclusion. Military service members are uniquely qualified for combat deployments, not civilians. The Uniform Code of Military Justice binds service members to follow orders and was specifically developed to aid warfighting in these environments. For good reasons, civilians are not bound to these same rules. Subsequently, we should never expect civilians to be forward deployed, particularly during conflict.

Second, many tech giants in Silicon Valley are not incentivized to contract with the DOD. Several have profitable business relationships with China, often preventing concurrent contracting with the U.S. military. Some companies cannot compete with the contracting advantages given to small businesses and protected class owners. Other firms cannot afford the professional assistance required to navigate bureaucratic barriers to government contracting, so they avoid it altogether. These hurdles have created a restricted market that does not fully benefit from free enterprise and optimal outcomes. This preventable course often yields ill-suited capabilities for conflict against our adversaries, something we cannot afford.

... dependence on vendor support during high-intensity battles may be unrealistic.

Offensive Cyber

Competition chiefly exists in the information environment, resulting in the development of the information maneuver occupational field that encompasses cyber, space, and influence operations. These professions were specifically established to address warfighting during competition. Highly specialized Marines serve in these niche billets, mainly in the National Capital Region, engaged in daily real-world operations. Similar existing MOSs (communications, signals intelligence, and communications strategy) generally have more traditional warfighting roles within the FMF, focused mainly on conflict rather than competition.

Cyberspace recently emerged as the primary warfighting domain within competition. This is predominantly because offensive actions in cyberspace do not seem to yield kinetic responses, but they do establish gains within the gray area, precisely meeting the objectives of competition. Offensive cyberspace capabilities are maintained at Fort Meade with U.S. Cyber Command and Marine Forces Cyber Command. The capability is split between joint operational requirements and the objectives of deployed Marine forces.

Within this model, MAGTF commanders do not have organic offensive cyber assets at their disposal. During the conflict phase, MAGTF commanders would leverage direct support relationships with Marine Forces Cyber Command to attain effects on targets. Assuming communications links to make this long-distance request are not compromised, there is still an unsatisfactory time lag in this reach-back model. This is a perfect example of how competition has erroneously taken precedence over conflict. In a high-intensity kinetic battle, MAGTF commanders need unity of command, not handshake agreements, to achieve their end states.

Moreover, cyberspace remains an overclassified warfighting domain. Classifications are meant to protect sources and methods. In most cases, general concepts do not need to be classified. These unnecessary restrictions on information sharing prevent commercial interests and academic professionals from advancing the body of knowledge in this field. The result is a mysterious, highly bureaucratic capability managed at the highest levels of the DOD.

This is satisfactory for the small group of cyber operators that independently engage the gray zone each day. However, a conventional conflict requires proper integration of all warfighting capabilities across all domains, and information sharing is vital to this fusion.

Civilian Workforce

Our government civilian information technology and acquisition workforces remain central to our warfighting mission's success. They are designed to augment military service members in daily stateside roles. They also provide leadership and continuity to absorb the shock of active-duty transfers and deployments. These workers' current hiring and retention practices are synonymous with those of a tenured university professor. Pay is generally fixed and unlinked from performance, and termination is extremely rare. These jobs were initially intended to promote the civil servant culture of American sacrifice, with benefits and job security in return. This Industrial Age system still has relevance in static, administrative jobs that depend on routine and repetition rather than influence and creativity. It is also adequate under the supervision of senior uniformed service members, a luxury that is had during competition but not conflict.

Unsurprisingly, this system does not work in IT fields. Success in IT requires more than assembly-line actions. Self-study, research, and blazing initiative are needed to keep up with this fast-paced field. Sadly, our stale and inefficient pay and performance structure has placed our IT civilians and procurement experts in disadvantaged positions. There is little financial or professional incentive for them to create cutting-edge solutions at the tempo of conflict. Consequently, they serve in non-essential roles that do not extract true potential, as evidenced during furloughs and shutdowns. The effect is contracted FMF solutions that bypass the formal acquisition process and resist dependence on government civilians. Examples include wireless LANs, high-speed satellite terminals, and cloud-based tactical data centers that are replacing tactical equipment at both stateside MEFs.

Way Ahead

The stated challenges can be overcome with simple changes. First, there can be no misunderstanding that service members make their unique contribution to America during conflict. Competition can be outsourced to civilians but conflict cannot. Though competition is preferred, preparation should weigh towards conflict, or else deterrence will fail. Our contract with America deserves no less.

The best deterrence for warfare is a force prepared for conflict, not one that is an expert in competition.

Second, commercial solutions must be adopted without dependence on physical vendor support during conflict. Marines must have the training and authority to locally repair, replace, or reconfigure systems and equipment as required. Cloud-based solutions cannot be a critical vulnerability. Instead, local "cloudlets," redundant transport, and versatile TTPs should seamlessly overcome a loss of any cloud capability. Furthermore, a streamlined contracting system should invite all businesses to compete fairly for DOD contracts in an open marketplace and incentivize them to do business with America rather than China.

Third, organic offensive cyber operations teams should begin training with MAGTFs, providing independent support. With the proper constraints, MAGTF commanders can utilize limited, organic offensive cyber capabilities to support greater maneuver efforts. In the case of personnel shortfalls, defensive cyber operators who already reside in the FMF can begin practicing these roles. Much like the evolution of electronic warfare capability delegation from strategic to tactical levels over the last 50 years, offensive cyberspace operations must follow the same course. In addition, a review of classification procedures within cyberspace operations should release the bureaucratic stranglehold that has unnecessarily plagued information sharing since the inception of the cyberspace domain. The total force can then become aware of this capability in preparation for conflict.

Fourth, our government civilians who manage and procure IT solutions should be hired and retained according to modern pay and bonus structures that incentivize performance rather than presence. Sharp bonuses that compete with the civilian technology sector should be awarded to those who seek autonomy and produce fast results. Employees should be encouraged to swap positions or move to the private industry every three years, facilitating the flow of new ideas. Local supervisors should freely define position descriptions and easily manage personnel without the fear of whiplash from bureaucratic officials. This streamlined employment process is used in large corporations, tech start-ups, and fast-food restaurants. We, too, can do better for our civilians.

Concluding Remarks

The best deterrence for warfare is a force prepared for conflict, not one that is an expert in competition. Our tactical maneuver force is aware of this, but our cyberspace technology efforts require more focus. Unlike many of America's former adversaries, today's peer threats have a cyberspace technology capability that rivals ours. Therefore, a reorientation of commercial technology procurement, offensive cyber capabilities, and civilian IT workforce incentives is now in order. Time is running out.

Author's Notes: Credit to the Hoover Institution's "Tech Track II" for inspiring this article.

AIRBUS U.S. SPACE & DEFENSE

Evolving an enduring platform for a revolutionary mission

Unmanned UH-72B Logistics Connector
In any clime and place.

AirbusUS.com

AIRBUS

The Planetary Metaverse and the Navy and Marine Corps Team

Meeting the challenges of the 21st century

by LtCol Christopher Tsirlis (Ret)

After recently retiring from the Marine Corps and joining a technology company, things look different from the other side of the fence. The degree of technological change and innovation is even faster than I thought. The rapid democratization of information and the increase in digital connectivity leads to a natural clash of cultures for hierarchical-based organizations like the Navy and the Marine Corps. The current culture of the Navy and the Marine Corps that drives innovation is often at odds with the culture of innovation and adoptive change that is driving the rest of society. The former relies on the expertise and experiences of the few, the latter depends on the shaping and technical acumen of many. Hence the Navy and the Marine Corps will continue to lag because innovation driven by a 20th-century organizational model will always struggle to meet the challenges of the 21st century where the marketplace decides what is best based on user preferences and value to the consumer. Since there is no true consumer-driven military marketplace for innovation, where the best ideas emerge because of bottom-up military market demand, external rapid technological changes will continue to dictate how the Navy and the Marine Corps respond and adapt to our adversaries' technical advancements in the future. The key is for the Navy and the Marine Corps cannot rapidly synthesize innovation from civilian global markets. How to change this fact is fundamental in advancing technology as an enabler. As VADM Rondeau (Ret) states, "Today, strategic competition is fundamentally an innovation race. To prevail, we must quickly secure technological advantage, as well as the cognitive agility to employ it effectively." She further explains that decision advantage is decisive in warfare and that, "Innovation, co-creation, and agility of mind and application have been and always will be essential factors in warfare. Cognitive agility is the intersection point of effect that brings knowledge to capability and provides decision advantage."[1]

>See bio on page 44.

Decision advantage sounds nice but enabling it with physical and virtual infrastructure is where the rubber meets the road. This requires a dramatic change in how we deliver information to support cognitive agility by moving from an on-premises data center model to a hybrid-cloud-based infrastructure model that leverages the best of what commercial technology has to offer. If both the Navy and Marine Corps continue to pursue an enterprise cloud-based data-centric architecture on commercially available cloud environments for both IL5 and IL6, the foundation will be set for some exciting and currently available technological advancements in the areas of gaming, exercising, modeling, and simulation (GEMS).

The recently published Marine Corps new doctrinal publication *MCDP 8* states, "The *information environment* is the global competitive space that spans the warfighting domains, where all operations depend on information. It includes information itself and all relevant social, cultural, psychological, technical, and physical factors that affect the employment of forces and bear on commanders' decision making."[2] With this definition in mind, let us examine how the information environment is changing in the world of serious gaming (aka, wargaming).

The Future is the Metaverse

One meaningful change has been how GEMS is beginning to transform the future of the internet which is increasingly called the Metaverse. There are many definitions of the Metaverse currently out there, and it is constantly being defined. However, here are a couple of good thoughts on what the Metaverse means and the changes that are coming to us all:

> "*The next wave of internet, the digitization of people, places and things and their interactions … enable you to build your own immersive worlds … that are accessible from anywhere or any device.*" Satya Nadella–Microsoft CEO.

Along the same type of thinking:

> "*The next generation of the Internet that is always real-time and mostly*

3D, mostly interactive, mostly social and mostly persistent." John Riccitiello–Unity CEO.

The metaverse then merges consumer, enterprise, and industrial information environments into a world that we may not recognize in a few years. When you think about it, the fusion of data, both structured and unstructured, allows for the conditions to process enormous data estates to support decision advantage in complex environments. This is where artificial intelligence and machine learning (AI/ML) come into the equation. Regardless of the medium, humans alone do not possess the ability to sift through these copious amounts of information and produce the insights necessary to achieve decision advantage. Therefore, AI/ML supports decision advantage that is centered on speed and accurate interpretation of copious amounts of information: to sense and then make sense of one's information environment and then most importantly to act in a way that achieves the desired effects of one's actions. The question is how does a warfighting organization like the Navy and the Marine Corps get there with the aid of technology? One way is using GEMS tools and metaverse-enabling technologies. Here, gaming takes on a new meaning where experimentation and campaign modeling enable a new world of possibilities.

Wargaming and Gaming Engines

GEMS technologies begin with 3D geophysical maps and terrain services which are nearly realtime accurate and enhanced to create realistic physic-based virtual environments enabled by gaming engines such as two immensely popular engines such as Unity or Unreal.[3] Remarkably, these gaming engines can utilize Entity Component Systems where over 10,000 attributes can be given to a single entity. For those who have used XBox games such as *Flight Simulator*, you get a sense of what type of realism can be shown to provide an immersive experience. Once these technologies are fused together and engineered into high-capacity cloud-based services, you now move from the metaverse to the Planetary Metaverse.

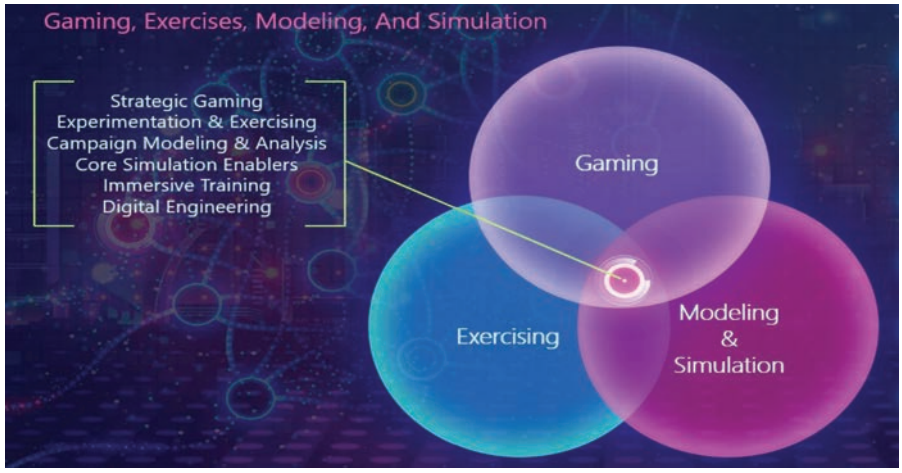


Figure 1. ***(Figure created by Christopher De Felippo, Chief Storyteller, Microsoft.)***

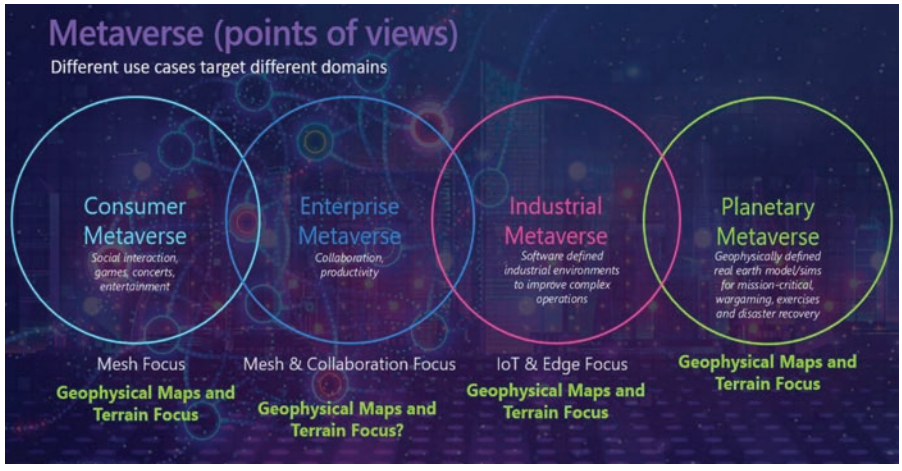


Figure 2. ***(Figure created by Christopher De Felippo, Chief Storyteller, Microsoft.)***

The Planetary Metaverse

The *Planetary Metaverse* is designed for mission-critical environments like combat simulations or disaster recovery. It enables the fusion of geophysical maps and terrain, modern collaboration technologies, digital twins, Internet of Things, and high-performance edge platforms to become extensions of an extensibility platform. There is a planetary metaverse building. The key question is how do we leverage it? One way is to take traditional wargaming and course of action analysis to levels never achieved before. With the right authoritative data sources, the Planetary Metaverse can be "fully informed"[4] whereby users can conduct wargames in near realtime scenarios that allow for detailed simulations to occur before a final decision is made. The Planetary Metaverse can allow wargame designers to capture and log analytics and then apply AI/ML models to examine probabilities of success, risk factors, and human factors before a course of action is decided. It is human-centric and aids cognitive decision making in complex environments. The 38th Commandant of the Marine Corps, Gen Berger, stated, "The National Defense Strategy has directed us to focus in new areas, and this requires us to think, innovate, and change. Addressing these new missions starts with ideas, ideas are developed into concepts, and concepts that are then tested and refined by wargaming, experimentation, and M&S."[5] The Planetary Metaverse supports these actions because an accurate representation of the operational environment integrated with realtime sensor networks and data analytics, we can continuously update the opera-

tional environment while simultaneously using the Joint Planning Process. The result is not only a better plan but a better rehearsal, execution, and debrief due to the near realtime nature of the operating environment. The mixture of people and technology must change to make better decisions which results in better cognitive agility and more fully informed decision advantages against our adversaries.

Stakeholders

There are several potential stakeholders in the Planetary Metaverse. As it pertains to wargames and war planning, the Planetary Metaverse can allow for distributed game players (blue, red, and white cell participants) to emulate strategic, operational, and even tactical-level actions in wargames. Depending on how the game is designed, they can simulate, analyze, and replay actions against a game clock. To capture key decision points and apply sentiment analysis which can provide insights into the way commanders and their staff respond to certain events. Further, the ability to analyze with machine learning models means actions can have artificial intelligence algorithms applied to provide optimized courses of action, both on the blue and red sides of the map. To understand and simulate the information environment, effects of a blue forces and adversary's weapons engagement zone and overlay electromagnetic capabilities over a 3D accurate geospatial terrain map brings decision advantage to another level for war planners. This is just one of the possible scenarios of this technology.

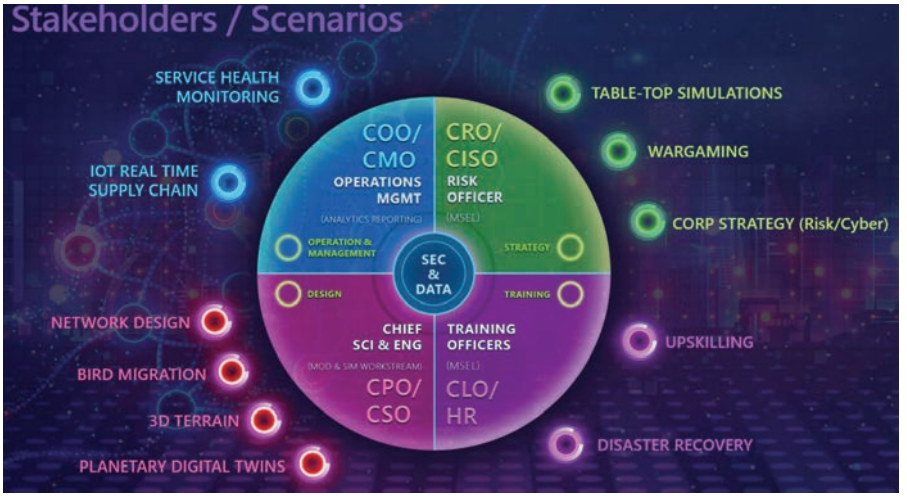


Figure 3. *(Figure created by Christopher De Felippo, Chief Storyteller, Microsoft.)*

Figure 4. *(Figure created by Christopher De Felippo, Chief Storyteller, Microsoft.)*

The mixture of people and technology must change to make better decisions which results in better cognitive agility and more fully informed decision advantages against our adversaries.

GEMS Tools and JADC2

Most importantly, the use of GEMS tools within the Planetary Metaverse construct helps address some of the most important desires of the DOD Defense Science Board (2021) and their efforts to close the gaps in the JADC2 strategy.[6] Whereby virtual exercising increases readiness and enhances warfighter lethality and survivability. The Planetary Metaverse directly addresses the line of effort 3 of the DOD JADC2 strategy by providing a data-driven fabric for "shared situational awareness, synchronous and asynchronous global collaboration, strategic and operational joint planning, realtime global force visualization and management, predictive force readiness and logistics, realtime synchronization and integration of kinetic and non-kinetic joint and long-range precision fires, and enhanced abilities to assess Joint Force and mission partner performance"[7] The modeling and simulation aspect of GEMS can directly address this and seeks to ensure that modern models support the requirements of the JADC2 strategy. It is also the only cost-effective way of training battle management algorithms at the sophistication required for decision advantage is going to be in the synthetic world by fusing data from the real world into it.

Summary

The Navy and Marine Corps can

prepare for this growing technological change and what the Planetary Metaverse has to offer by first establishing a single integrated IL5 and IL6 hybrid-cloud network for both enterprise and tactical use. Establish a modern identity and access management policy and zero-trust architecture that ensures security and moves from an on-premises data center model to a hybrid-cloud-based infrastructure model that leverages the best of what commercial technology has to offer. Continue to invest heavily in robust transport (terrestrial and celestial) infrastructures, equipment, and experiments daily. This bedrock cloud-based data estate can provide the type of realistic simulation environments that really evaluate operational ideas and concepts through planning and wargaming using realtime 3D spatial environments the Planetary Metaverse can provide. Lastly, the Navy and the Marine Corps must create a business model where models and assets of all kinds can be tokenized and used in a pay-for-play construct and thus thrive in a digital marketplace within the Planetary Metaverse. Only then will the Navy and the Marine Corps be able to position themselves to be able to fully adopt GEMS tools and begin to fully realize the DOD strategy for JADC2 and further the cognitive agility of its forces and maintain decision advantage against our adversaries.

Notes

1. Ann Rondeau, "Rebalancing the Science and Art of War for Decision Advantage," *Proceedings* 148, No. 8 (2022).

2. "Metaverse has also been called '3D Internet.'"—Unity's head of Government Solutions, John Cunningham.

3. Gaming engines definition: A game engine is a software framework primarily designed for the development of video games and includes relevant libraries and support programs. The "engine" terminology is like the term "software engine" used in the software industry.

4. Fully Informed means it can be fused with realtime or near realtime data sources (classified or unclassified).

5. Megan Eckstein, "Marine Planners Using Commandant's Guidance to Start Crafting Future of the Corps," *USNI News*, September 18, 2019, https://news.usni.org/2019/09/18/marine-planners-using-commandants-guidance-to-start-crafting-future-of-the-corps.

6. Defense Science Board, January 2021, GEMS Executive Summary FINAL.pdf (cto.mil).

7. Department of Defense, *Summary of the JADC2 Strategy*, (Washington, DC: 2022).

The Marines' Startup

Creating a culture of innovation in a maneuver manner

by GySgt Jeremy A. Kofsky & 1stLt Carter McCausland

The Marine Corps is the most innovative of the Services: it is enshrined in doctrine, constantly extolled by leaders, and several organizations exist to drive this innovation and provide the Marines on the forward edge with the leading edge of technology and procedures. Similar small-unit efficacy is seen daily in Go-Pro footage from Ukrainians along the Donbas trench line and the hamlets and fields of Zaporizhzhia, Ukraine. From the use of drones to battlefield manufacturing and improved tactics, the innovation of the numerically inferior Ukrainian military has blunted the sledgehammer of the supposedly invisible Russian military juggernaut. However, if similar innovation were tried in the Marine Corps, despite the innovative culture embiggened within Marines, it would encounter untold resistance; one need only look at the *Force Design 2030* debates to see what any shift from the norm portends from structural equities within and without the Marine Corps.

While there are many reasons for structural lethargy built within the Marine Corps bureaucratic technology centers and acquisition fields, there also needs to be a balance between the need for larger (DINOSAUR) programs and nimbler tactical-driven innovations. By adopting the strategy of the free-market start-up, the Marine Corps can live up to its true innovative culture and apply maneuver warfare edicts to appropriately support an innovation ecosystem within the Marine Corps that is dynamic, proactive, and, above all, sustainable. This maneuver warfare analogy is specifically apropos as several innovative companies still have *MCDP 1* as a foundational document to spread innovative underpinnings throughout their organization.

>GySgt Kofsky is an eighteen-year veteran of the Marine Corps with master's degrees in both International Relations and Public Policy (Terrorism, Peace, and Mediation). He has deployed eleven times with six combat tours. He is currently assigned as a Parachute Operations Chief for 2D Intelligence Battalion at II MEF Information Group at Camp Lejeune, NC.

>>1stLt McCausland is an Intelligence Officer with 2d Intelligence Battalion. He has eight years of experience in venture capital as a Founder, General Partner, and Board Member at two investment funds and manages over ten million dollars in assets.

Innovation ecosystems take on many types and stripes. The baseline definition of an innovation ecosystem is "the evolving set of actors, activities ... and the institutions and relations, including complementary and substitute relations, that are important for the innovative performance of an actor or a population of actors."[1] This wide-ranging definition has resulted in different versions of ecosystems, all possessing unique from "place-based" to "distance-modeled" ecosystems. The end goal is the same: create innovations to support grassroots and eventually wide-spectrum activities. The use of systemic programs of record at the larger headquarters level is still important, but similar to how IBM still relies on the latest Silicon Valley startup to drive their own research, the Marine Corps should endeavor to create and formulate an innovation/startup culture that begins at the fireteam level and halts to catch fire from there.

Operational Planning

The six essential elements to create an innovation ecosystem are:

1. Set the Aspiration and a Bold Vision.
2. Cluster and Partner Strategy.
3. Capital and Funding Venture Capital, Business/Academic Research and Development, Federal Funding.
4. Talent and Community Building.
5. Real Estate, Infrastructure, and Place Making.
6. Diversity, Equity, and Inclusion.

While these techniques were developed mainly to support the private sector, they can also be hugely successful in the government and public sector, despite the bureaucratic slowness inherent within these organizations.

Set the Aspiration and a Bold Vision

The Marine Corps has already set the conditions on several of the essential elements, but the further flourishing of the innovation ecosystem requires an adherence to the spirit of maneuver warfare principles. The element of *Set the Aspiration and a Bold Vision* has already been codified and expounded upon by *Force Design* and expeditionary advanced basing operations. Sundry attachments and annexes to cover issues like talent management, installations and logistics, training and education, and their concepts for employment, namely the Stand-In Forces Concept, further reinforce the principles and create concrete examples to launch innovation with aspirational endpoints, intent, and maneuver room for people to innovate within those areas.

Cluster and Partner Strategy

Understanding the various organizations that can support initiatives with specialists and innovators outside an internal organization allows for a bespoke tailored approach to innovation to have ideas be matured and incubated while still in the not-fully developed space. One of the largest failings of innovation in the military is the innate desire to have a fully formed idea by one person/small group and, if at any step of the way, there is hesitation or an unanswered question, then approval can be automatically withdrawn and innovations have to be started from the ground up. The military is filled with literally hundreds of thousands of brilliant people; would a smarter strategy not be to allow these groups a mechanism to collaborate and utilize *yes and* collaboration methodologies?

Capital and Funding

Typically, the reason ideas and innovation die in stasis is they do not fit into a proper line item, budgeting cycle, or are not the right "color" of money. While there needs to be controls on budgeting to prevent boondoggles and other forms of malfeasance, the innovation sphere requires innovative budgeting mechanisms so people can be allowed to succeed by failing. Becoming better costs money and aligning generalized "innovation" budgeting through either research and development funding, public/private through research agencies/universities, and/or operations funding are potential ways to increase investments. The DOD should be thought of as a venture capital or "investment angel," and the Marines, as the "founders" or "executive members," have a fiduciary duty to give both the DOD and their Marines an accurate picture of where their capital is best placed for maximum returns.

Talent and Community Building

Bringing together diverse talent is important, but so is the ability to make talent that feels hidden visible to others. The radio operator and micro-miniature radio maintainer can create commercial off-the-shelf signature management detectors; they just need to know

Bringing together diverse talent is important, but so is the ability to make talent that feels hidden visible to others.

they can. They have the talent, training, and want to do great things; what they lack is a marshaling force to harness them into a collective team. This is where a collaborator, fusion expert, or project manager can be indispensable as they can provide this oversight, enable collaboration, and identify those hidden talents within an organization. This should be a typical role of a leader in an organization but sometimes gets buried under the minutiae of day-to-day tasks, and it is a learned skillset. Having project management, lean six sigma, or other project oversight programs as part of regular professional military education can go a long way in improving this underutilized and critical component of innovation.

One of the best examples (and at the institutional level, the only) of this type of organization currently in the Marine Corps is the Marine Innovation Unit. The Marine Innovation Unit's novel approach is they take a litany of hyper-intelligent and successful reservists with backgrounds in some of the best tech companies, consulting firms, and research institutions in the world and throw them against some of the Marine Corps' biggest issues. The novel part of this is there is no real rank structure within the working groups (the unit is still a Marine Corps unit and adheres to Marine Corps customs and courtesies), good ideas win out; these Marines choose their assignments and work with their overall program manager to align their interests and skills to specific problems; and collaboration happens remotely where the Marines live so they can best focus on idea formulation and collaborative solutions vice a regimented planning cycle.

Real Estate, Infrastructure, and Place Making

Having innovation campuses is another critical aspect of a successful innovation ecosystem. While remote work can work in hyperspecialized areas, breaking down walls and dragging out ideas is best done in a room with a bunch of whiteboards and plenty of black coffee. The II MEF Innovation Campus and the 1st Maintenance Battalion's Innovation Manufactory are examples of this and allow for the quick creation, optimization, and production of smaller-scale ideas, typically of a tactical nature fitting neatly within the Marine Corps' overall mission statement of tactical excellence creating strategic effects. Increased use of these areas and the continued springing up of innovation campuses throughout Marine Corps bases will likewise increase returns on investment and allow for more solutions in a start-up model mode.

This warrior spirit of innovation continues today ...

Diversity, Equity, and Inclusion

As discussed in earlier sections, varied and disparate skill sets are needed to make a lot of the modern innovations the military needs. They also need to have a variety of experiences and backgrounds. Similar to how a person from the city will likely not know about issues with wildlife and farm animals, a person from the country will likely not understand the cacophony of noise and people associated with an urban setting. Both of these would be able to contribute in equal ways to reconnaissance equipment designed to work in both areas, however. A person brand new to the Marine Corps likely has no preconceived biases about the Marine Corps limitations and, therefore, can look at a problem with a naïve level of genius a senior NCO or officer may lack simply by their inculcation in the Marine Corps. Balancing all these differences creates a more holistic process and product/innovation in the end.

Silicon Marines?

The beauty of the Marine Corps is anything is, within reason, capable of happening due to the organization's ethos on mission accomplishment above all. In terms of the specifics of a professional military education program within a unit that emphasizes maneuver warfare, one needs both codified and zealotry to accomplish the objective. Having a return on investment and showing the usefulness of thinking Marines is key. Once a decision is made to begin an innovation program, a capable cadre of instructors needs to be recruited and mentored to a standard. Achieving buy-in from leadership is another critical aspect of this operation. If Marines see they are merely doing this for the learning experience, but the command really does not care, then the program will die on the vine. Leadership carving out time for classes and building maneuver warfare into their operations will enable a nimbler organization, and people will begin to see the successes of the Innovation process and, therefore, will want to build on it. Sustainment might be the hardest part of this as the program has to last past the initial cadre; otherwise, it was merely a cult of personality and not a program.

The drive for innovation is as old as combat; since the days a Neanderthal figured out a rock was more effective than bare hands. The Neanderthal did not have to go through a series of program boards, budget cycles, and other "necessary" processes. They figured out what worked for their situation, used it, and discussed it around the campfire with their tribe. This warrior spirit of innovation continues today but is bogged down in the best-intentioned programs of the Pentagon. The future success, and indeed lives, of those in the future trenches, atolls, and fjords of combat in the next battles deserve the ability and the support to innovate in a manner more violent and quicker than those opposing them. Let's give them those tools and be amazed by the outcome.

Note

1. Ove Granstrand and Marcus Holgersson. "Innovation Ecosystems: A Conceptual Review and a New Definition." *Technovation*, November 26, 2019, https://www.sciencedirect.com/science/article/pii/S0166497218303870.

POLARIS

MRZR ALPHA

THE MARINE CORPS ULTRA LIGHT TACTICAL VEHICLE

MODULAR. INTERNALLY TRANSPORTABLE.

MISSION READY.

POLARIS | GOVERNMENT & DEFENSE

military.polaris.com

Space & Cyber

Combined-arms capabilities for the conflict phase of warfare

by LtCol Arun Shankar

The space and cyber warfighting domains have emerged and been formalized now for nearly a decade. Both domains are associated with newly formed combatant commands, and the space domain even has its own associated Service. Despite this, many tactical commanders still lack a comprehensive understanding of integrating these domains into traditional conflict. Aside from the theoretical knowledge that these domains underpin both friendly and adversary command and control, several tactical commanders know little else. This article distills cyber and space into digestible concepts for tactical commanders while also proposing ways to improve the employment of these combined-arms capabilities during the conflict phase of warfare.

Background

Space and cyber roles and responsibilities are categorized similarly into offensive actions, defensive actions, and daily operations.[1] Offensive operations target the adversary, defensive operations focus on protecting friendly capabilities, and day-to-day operations involve operating and maintaining satellites and computer networks. U.S. Space Command (USSPACECOM) and U.S. Cyber Command (USCYBERCOM) are the warfighting combatant commands (CCMD) that have operational responsibility for these domains. They perform independent missions as well as provide support for other CCMDs.

>See bio on page 70.

Due to the abstract nature of computer networks, USCYBERCOM centrally manages many of its roles, including offensive cyberspace operations. Moreover, there is an overarching demand to centralize computer network domains under one joint umbrella, rather than by the individual Services. Consequently, this would aggregate defensive operations and daily maintenance operations at USCYBERCOM, leaving little authority to tactical commanders. USSPACECOM has a similar approach, aiming to centralize global satellite operational management under one umbrella, tactically operated by the U.S. Space Force (USSF). Though the other Services provide component commands to USSPACECOM, their relevance is negligible compared to the USSF.

This aggregation of resources ... stems from a realization that space and cyberspace are independent warfighting domains that require global resource management.

This aggregation of resources in both CCMDs stems from a realization that space and cyberspace are independent warfighting domains that require global resource management. The focus on centralized ownership of these domains is akin to the emergence of the Strategic Air Command and the eventual transition to the Air Force in 1947. In short, it was rightfully believed that airpower was a strategic asset in its own warfighting domain, able to operate independently of ground warfare to achieve strategic gains. Since 1947, we have seen numerous air operations achieve such outcomes.

Part of this strategic role is the establishment of air superiority—ensuring air activities are conducted without prohibitive enemy interference. Similarly, USCYBERCOM and USSPACECOM have strategic responsibilities in establishing cyber and space superiority, independent of any adjacent warfighting mission. Specifically, the competition phase of warfare (Figure 1 on the following page) is dominated by the space and cyber warfighting domains, where most actions derive strategic value.

Consequently, it can be said that USSCYBERCOM and USSPACECOM operate at the operational level of war. They bridge national policy and tactical actions through campaign planning. Actions at the operational level have a strategic impact, hence the link to strategic goals. They also contribute to the global integration of all CCMD efforts and support global campaign plans.

Space and Cyber within the Marine Corps

Present State. Space and cyber capabilities have only recently been introduced to the Marine Corps. Restrictions on capabilities and authorities prevent the full use of these capabilities at the tactical level where the FMF resides. Offensive cyber capabilities almost solely reside at or near USSCYBERCOM within the Marine Corps Cyberspace

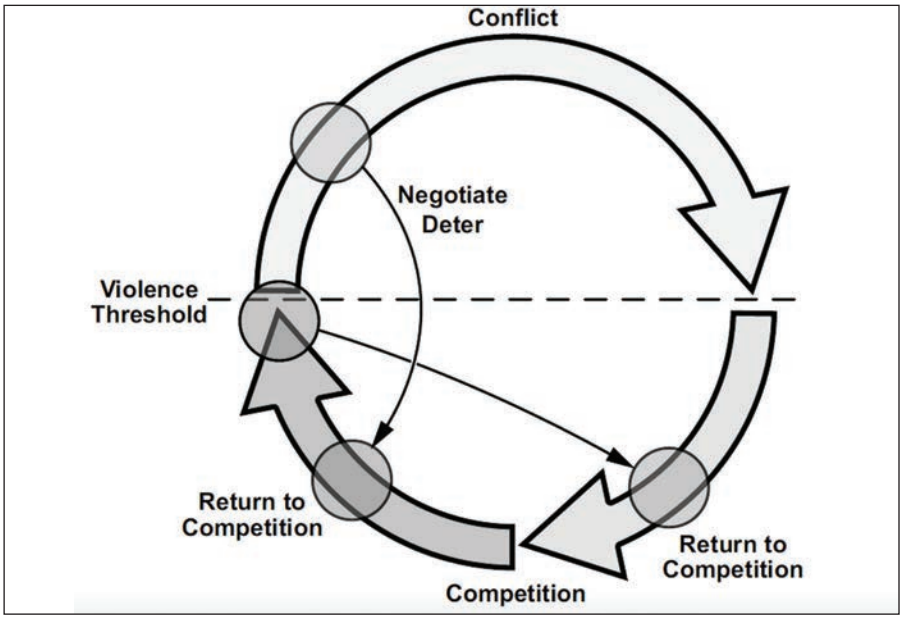


Figure 1. Conflict vs. Competition* (MCDP 1-4).** *(Source:* **MCDP 1-4 Competing.)*

Warfare Group in support of their operational mission. Defensive cyber operators reside within the Service at the Marine Corps Cyberspace Operations Group and the communications battalions. Daily operations are performed by the long-standing communications MOS community. Offensive and defensive space capabilities are similarly distributed between USSPACECOM and the FMF but on a much smaller scale due to equipment costs and the dominance of the USSF.

The MEF Information Group aggregates all information-related capabilities for the FMF in each of the three MEFs. As a result, the bulk of space and cyber capabilities within the FMF reside within these formations. Space and cyber planners liaise with the Marine Corps Information Command (MCIC), where effects can be requested. They also serve as resident subject-matter experts for the MEF Information Group and MEF commanders.

Marine Corps Forces Cyberspace Command (MARFORCYBER) holds most of the Service's cyber capability. As a Service component to a CCMD, its capabilities are rightfully prioritized and centralized at USCYBERCOM. Organic and attached Marines are provided exceptional training and real-world experience while in support of gaining and maintaining cyberspace superiority. They also provide defensive capabilities on the Marine Corps Enterprise Network (MCEN).

Conversely, Marine Corps Forces Space Command (MARFORSPACE) maintains a planning capability, distributing most space professionals and assets to the FMF. In essence, this model is the converse of MARFORCYBER, which is focused on enabling the FMF to eventually support geographic combatant commanders. Moreover, the Army, Navy, and Air Force have recently shifted most of their crucial space capabilities to form the USSF, significantly reducing their own force offerings to USSPACECOM. As a result, the USSF provides the overwhelming majority of space capabilities to USSPACECOM, dominating the culture and execution of the mission.

Future State. Optimally, Marines desire the use of space and cyber capabilities as combined-arms assets during

the conflict phase of warfare. After all, many of the tradeoffs that resulted in Force Design were predicated on these assumptions. However, the Corps' recent campaign of learning has revealed that this tactical employment of space and cyber capabilities is easier said than done. This future state will require changes in strategic policy and Joint Force operations.

First, the Marine Corps should gain offensive space and offensive cyberspace capabilities and authority at the tactical level. *To be clear, this means that O-5 and O-6 level commanders should have the personnel and resources to execute offensive space and cyberspace actions without reach-back support*. Specifically, Marine Corps commanders charged with distributed, decentralized, stand-in force missions need these resources more than ever before. Awaiting these means when conflict eventually demands them is too late. Commanders cannot realistically understand these capabilities unless they practice exercising them in an authentic, expeditionary manner. Once these resources are granted, the MEF Information Groups should expand their support beyond the MEF command element. They should train and educate O-5 and O-6 level commanders on using cyber and space capabilities as truly tactical, combined arms weapons during conflict.

Second, *we must acknowledge that space and cyber are not only tactical combined-arms capabilities but also strategic capabilities that can be planned and executed at the operational level of war*. The Marine Corps' contribution to this effort is the presentation of forces and capabilities to USSPACECOM and USSCYBERCOM. These CCMDs will use these capabilities to achieve space and cyberspace superiority, independent of FMF operations. Though this model isolates some Marines from their traditional warfighting roles and culture, it is a necessity to ensure the Marine Corps makes a proper contribution to the overall Joint Force. There is precedent for this, as we make similar concessions with Marine Security Guard requirements and the staffing of Marine Special Operations Command operators.

Third, *the dominance of the USSF in the space domain should be reexamined*. The USSF creates dilemmas for space contributions from other Services. In the present model, USSPACECOM headquarters is staffed by each military branch, but the overwhelming subordinate component contributions are from the USSF. This is not an optimal joint warfighting model. Perhaps a standard like USSCYBERCOM should be examined, where Service component members are trained by USSPACECOM entities to perform missions presently only assigned to the USSF. For instance, sailors, soldiers, Marines, and airmen could be trained to be satellite operators and subordinate commands could be reorganized to accommodate these truly joint contributions. In this way, space contributions are shared more evenly among the branches, and service members return to their individual Services with unique skills and experience that can benefit the greater Joint Force.

... tactical commanders must know how to seize superiority in these warfighting domains and return fire with accuracy and precision.

Fourth, *the specialized nature of space and cyber occupational fields is much more suited for restricted officer assignments than the current unrestricted officer manning model*. Instead of shoehorning unrestricted officers into these MOSs by fantasizing about analogous career paths, we should reconsider using warrant officers and limited duty officers to fulfill these duties, much like the Army does with helicopter pilots. Perhaps these officers can be commissioned through a similar path as unrestricted officers but designated on a restricted career path from their inception. In this way, there is no need to inundate boards with endless precepts and the creation of O-5 level "commands" to keep these officers competitively promoted. In the event that unrestricted officers are needed to laterally move from other MOSs into the space or cyber communities solely for leadership roles, warriors with deployed experience and former command roles should be chosen before officers looking for quality-of-life improvements and future civilian employment. These budding occupational fields deserve our best warfighters leading the way.

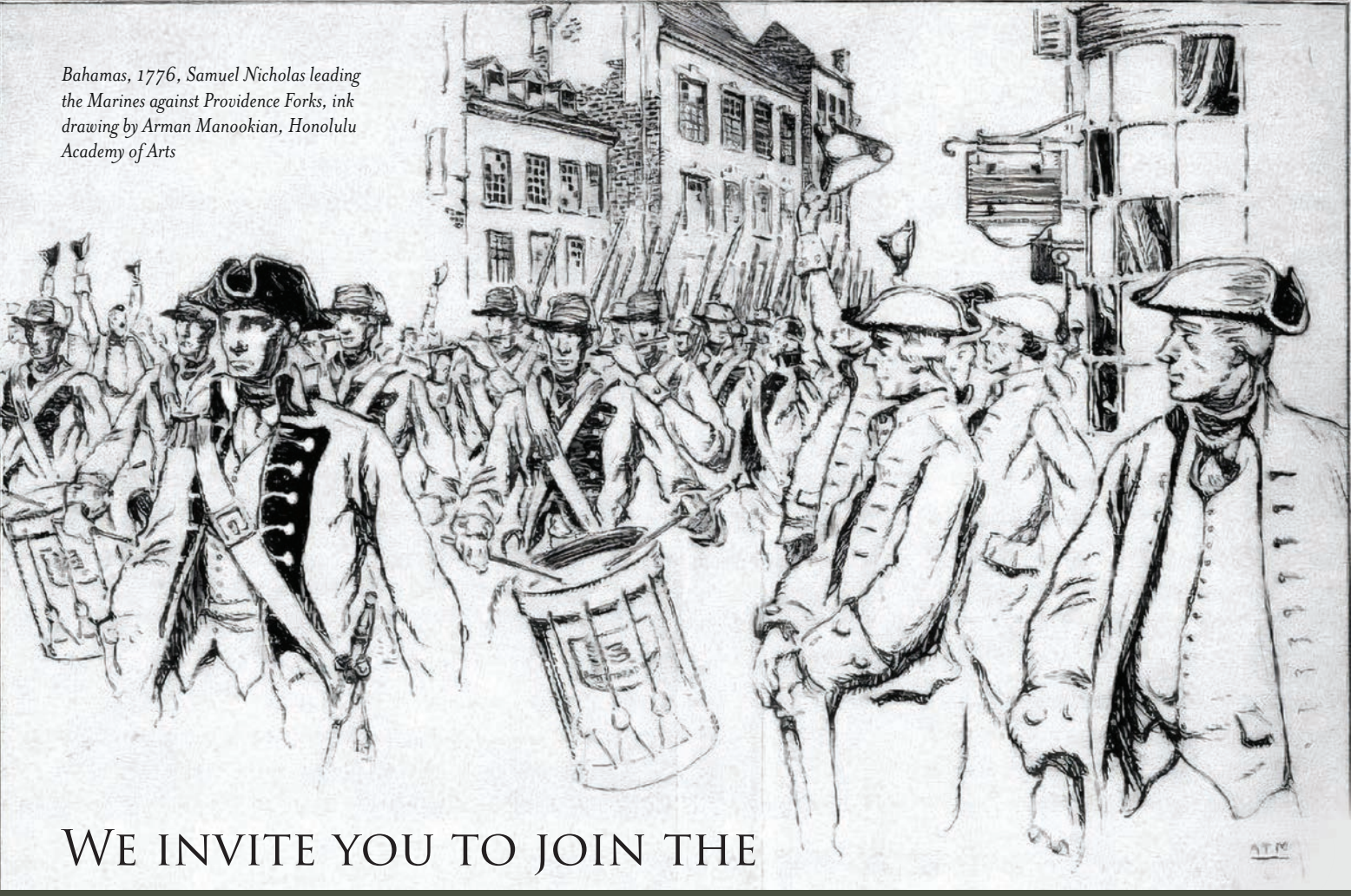
Concluding Remarks

The space and cyberspace capabilities mandated by Force Design have not yet been fully realized. Our campaign of learning has revealed many challenges with full implementation within the FMF. Central to this is a lack of capabilities, resources, and authorities to execute offensive space and cyber actions at the tactical level. Moreover, to satisfy Joint Force requirements and FMF demands, the Marine Corps must create resources for both mission sets, acknowledging that they do not overlap in most cases. Relevant contributions to the space superiority mission are complicated by the creation of the USSF and its overmatched presence within the domain. Lastly, restricted officers should fill most billets in these occupational fields, as there is no reasonable way to create an analogous career path for unrestricted counterparts.

Until these changes can be achieved, future exercises should incorporate space and cyber effects at a granular level, forcing commanders to truly understand these targeting processes and the consequences of decisions. White carding space and cyber is no longer acceptable, and neither are passive defensive scenarios that force commanders into degraded communications environments. Instead, tactical commanders must know how to seize superiority in these warfighting domains and return fire with accuracy and precision. We must move quickly—the lethality of our force depends on it.

Notes

1. Department of Defense, *JP 3-12, Cyberspace Operations,* (Washington, DC: 2018).



Bahamas, 1776, Samuel Nicholas leading the Marines against Providence Forks, ink drawing by Arman Manookian, Honolulu Academy of Arts

We invite you to join the

Samuel Nicholas Society

The Samuel Nicholas Society is named for the first commissioned officer in the United States Continental Marines and by tradition considered to be the first Commandant of the Marine Corps.

The Society honors those who have made a legacy commitment to the Marine Corps Association Foundation. Such a legacy is just one more way Marines continue to embody our core values of honor, courage, and commitment.

"The Marine Corps was my first real family. Consequently, I feel an obligation to repay the Corps by leaving something for other young Marines…I've been extremely fortunate, which I owe to the Marine Corps."

— Capt Ed McCourt, USMC (Ret)

For more information, visit

www.mca-marines.org/legacy-gift-planning/samuel-nicholas-society

If you have already included MCAF in your will or estate plan, please let us know. We want to thank you for your commitment of remaining always faithful to our Marines.

MARINE CORPS ASSOCIATION FOUNDATION

Effective Naval Integration Starts with Naval Education

Building a stronger blue-green team

by Maj Daniel J. Crain

"The changing character of war demands we educate and train our Marines with the most relevant and contemporary doctrine." [1]

—Force Design 2030 Annual Update, *June 2023*

>Maj Crain is a Marine Infantry Officer currently serving as a Course Manager and Amphibious Warfare Tactics Instructor (WTI) at Expeditionary Warfare Training Group-Atlantic (EWTGLANT). His current focus is training and educating Navy and Marine Corps staff members in amphibious operations and naval integration.

Marine Corps force modernization initiatives, emerging concepts, and real-world conflict and competition have increased the demand for closer Navy and Marine Corps integration. Integrated commands, such as Task Force 61/2 Naval Amphibious Forces Europe/2d MEB, have become commonplace in FIFTH, SIXTH, and SEVENTH FLEET task organizations, along with experimentation of Marine littoral regiments and MEUs supporting naval operations, activities and investments. These commands' operations, activities, and investments greatly increase the requirement that Marines understand naval and joint tactics, techniques, and procedures while also broadening staff member vernacular and Service cultural understanding across the Naval Services. To clarify upfront, integration throughout the rest of this article will refer to Navy and Marine Corps staff members working in close coordination, within a maritime task organization, to facilitate sea power on behalf of their common superior's objectives (i.e. Joint Force commander, Joint Force maritime component command, FLEET commander, or combined task force).[2]

With the increasing requirement for naval integration, demand for education regarding naval operations and integration has also risen. The expeditionary warfare training groups (EWTGs) receive numerous requests for training support and formal course offerings from staffs ranging from Echelon VI commands (battalions/squadrons) to Echelon II commands (Service components). These requests for training and education typically span topics ranging from the planning process to emerging concepts as described in *Force Design 2030*.[3] Ultimately, commands are seeking to increase their staff's shared understanding of Service cultural differences, the synchronization of effects in support of the FLEET and Joint Force maritime component commander, and overarching support to emerging concepts and real-world operations, activities, and investments.

Though widely unknown across the Marine Corps, courses exist to prepare Marine staff members to integrate with their Navy counterparts, but a clearly defined staff training continuum outlining billet requirements does not and thus must be codified and implemented. Stated simply, unlike the Navy, the Marine Corps generally does not mandate formal course attendance for staff billets. Instead, the Marine Corps relies almost entirely on the Commandant's Professional Entry and Intermediate-Level Education Boards to be the sole educator on topics such as amphibious operations, naval integration, and emerging naval concepts. This results in a variety of experiences based on modality (seminar vs resident programs) and fully disregards the enlisted ranks of the Marine Corps.

Conversely, within the Navy, commanders of U.S. Fleet Forces and U.S. Pacific fleet direct pipeline and fleet response training plan (completion for all carrier strike groups, expeditionary strike groups, amphibious ready groups, destroyer squadrons, composite warfare commander and warfare commander watch teams, as well as prospective carrier strike groups/expeditionary strike groups commanders).

This training is specifically directed in the strike group training continuum.[4] Many of the courses listed within this policy are open to Marine enrollment and span topics related to Composite Warfare Commander construct, fleet organizations, amphibious doctrine, and naval concepts such as distributed maritime operations, littoral operations in a contested environment, and expeditionary advanced base operations.

To be clear, the Marine Corps does recommend specific course attendance for MEUs through orders such as the "Standard Operating Procedures (SOP) For Marine Expeditionary Units (MEUs)" and the "Marine Expeditionary Unit (MEU) Pre-Deployment Training Program (PTP)."[5] However, these orders do not specify billet attendance, nor do they include courses oriented toward naval, expeditionary, or amphibious operational education.

Formal training and education commands, such as the EWTGs, recognize that the changing character of war requires closer Navy and Marine Corps integration across the discipline of naval education. Marines assigned as staff members must understand naval integration and interoperability earlier, but far too often this necessity is overlooked until the commencement of exercise planning, unit composite, or worse still—deployment. The Marine Corps path toward naval integration at the staff level must start with naval education through formal course completion. It should start in the classroom where Marines learn emerging concepts, shared doctrine, cultural nuances, and common vernacular.

As already highlighted, a blueprint for naval education and commander and staff is available and actively used across the broader Navy surface fleet. With this in mind, the Marine Corps should establish a standardized MAGTF command element staff training continuum. This training continuum would direct formal course requirements for individual staff members assigned to MAGTF command elements integrating within maritime task organization (i.e. Navy and Marine Corps operational fleet forces).

"The era of near-peer and peer adversarial challenges across the spectrum of the maritime domain is upon us, and the integrated Naval Force is preparing to meet them. The challenges that exist when fighting in the open oceans, within island chains, and into the littorals are causing a resurgence in tactical prowess and discussion within the Navy and the Marine Corps. The future fight dictates that both services are undoubtedly tied to each other and the intertwined integration needs to permeate all facets of manning, training, and equipping."[6]

... the changing character of war requires closer Navy and Marine Corps integration ...

To better educate Marines, the opportunity exists for the development of a training continuum directing formal course requirements for staff members assigned to MAGTF command elements who may integrate within a maritime task organization. Its objective should not be to dictate required training to achieve a certain type of certification (i.e. deployment or joint task force certification) but rather to specify courses staff members must attend to be most successful within an integrated command element.

The Marine Corps, writ large, lacks knowledge of the numerous Navy courses and commands that exist to support the development of staff members and prepare them for Navy-Marine Corps integration. These formal schoolhouses span the EWTGs, tactical training groups, Surface and

Theodore Roosevelt and Makin Island Expeditionary Strike Force. *(Photo by Petty Officer 3rd Class Brandon Richardson.)*

	Supporting Arms Coordinator Course - EWTG	Fire Support Development Course (FSDC) - EWTG	Tactical Air Control Party Course (TACP) - EWTG	Maritime Fires Course - TTGL	Tomahawk Tactical Commanders Course (TTCC)	Joint Targeting Staff Course - Joint Targeting School (JTS)	Collateral Damage Estimation - Joint Targeting School (JTS)	Maritime Staff Planners Course (MSPC) - TTGL	Warfare Commanders Course (WCC) - TTGL	Joint Operational Design Course (JODC) - CYBERCOM	Amphibious Airspace Operations Course (AAOC) - EWTGL	Amphibious Warfare Staff Planners Course (AWSP) - EWTGL	Amphibious Warfare Indoctrination Course (AWI) - EWTGL	ARG/MEU Staff Planning Course (AMSPC) - EWTGL	Senior Amphibious Warfare Officer Course (SAWOC) - EWTGL	Naval Expeditionary Operations Planners Course (NEOP) - EWTGL	Maritime Operational Planners Course - Naval War College	Maritime Prepositioning Force Staff Planning (MPFSP) - EWTGL	Afloat Knowledge Manager Course (MKMC) - EWTGL	Maritime Engagment and Crisis Response (MECR) - EWTGL	Maneuver Warfare Course (MWC) - TTGL	Environment Planners Course (SOPC) - EWTG	Senior MAGTF Operations In The Information Practitioner Course (MOPC) - EWTG	MAGTF Operations In The Information Environment (AMW WTI) - SMWDC	Amphibious Warfare Tactics Instructor Course - ASW/SUW WTI - SMWDC	Information Warfare (IW) WTI - NWDC	Maritime ISR (MISR) - NAWDC
Commander										X						X	X	X										
Deputy Commander										X						X	X	X	X		X							
Executive Officer										X						X	X	X	X		X							
Senior Enlisted Advisor										X						X					X							
Adjutant												X	X	X	X						X							
Administrative Chief												X	X	X							X							
Intelligence Officer	X					X	X			X		X	X	X	X			X										
Assistant Intelligence Officer	X					X	X																					X
Intelligence Chief																											X	
Operations Officer				X						X					X			X			X							
Assistant Operations Officer											X							X		X						X		
Operations Chief				X					x	X	X				X			X										
Asst Operations Chief												X	X	X									X					
Logistics Officer										X					X			X		X	X							
Assistant Logistics Chief													X	X												X		
Future Plans Officer									x	x	x				x				x									
Logistics Chief																												
Mobility Officer												x	x	x	x			x			x							
Communications Officer									x	x		x	x	x	x			x										
ComStrat Officer												x	x	x	x			x										
Staff judge Advocate (SJA)													x	x	x			x										
Information Management Officer (IMO)												x	x	x	x								x					
IO Planner																								x	x		x	
Fires and Effects Coordination Officer (FECC)	x	x		x		x	x	x	x			x	x	x	x			x						x				
Target Acquisition Officer	x	x			x	x	x				x																	
Air Officer	x	x	X	x		x						x	x	x	x													x
Reconnaissance Officer												x	x	x	x													

Figure 1. *(Figure provided by author.)*

Mine Warfare Development Center, Naval Aviation Warfare Development Center, and Naval Information Warfighting Development Center—to name only a few. The following staff training requirements (Figure 1.) is a proposed starting point for further development of such a training continuum.

Similar to the Navy's approach, training courses should be completed before Marines report to their newly assigned duty station and be scheduled in conjunction with permanent station change of duty orders and receive priority for quotas.[7] That said, completion of courses may be influenced by many factors such as existing prospective educational and Service background experience, available training time, and the training event schedule.

As the Marine Corps returns to its roots as an FMF and looks to integrate more fully into a naval expeditionary force, the EWTGs and numerous other schools are postured to support those endeavors in a multitude of areas. The personnel, experience, and training across Navy, Marine Corps, and joint schools are ready to meet the intent of both the Chief of Naval Operations and the Commandant of the Marine Corps force guidance. That said, knowledge starts with awareness of what training and educational opportunities already exist. Implementation of a staff training continuum allows the Marine Corps to fully harness the expertise that is readily accessible and better prepare MAGTFs for integration with the Navy and the broader Joint Force.

Notes

1. Gen David H Berger, *Force Design 2030, 2023 Annual Update*, (Washington, DC: June 2023).

2. Office of the Joint Chiefs of Staff, *JP 3-32 Joint Maritime Operations, Incorporating Change 1*, (Washington, DC: 2021).

3. *Force Design 2030, 2023 Annual Update.*

4. Commander, U.S. Fleet Forces Command, Strike Group and Staff Tactical Training Continuum, *COMUSFLTFORCOM/COMPACFLT INSTRUCTION 1500.49,* (Norfolk: 2022).

5. CG, II MEF, II Marine Expeditionary Force Order 3100.3E, (Camp Lejeune: 2018); and CG, 1 MEF, *I Marine Expeditionary Force Order 3120.9A,* (Camp Pendleton: 2017).

6. Col T.F. Kisch, *Academic Year 2024, Course Catalog*, (Norfolk: 2024).

7. Tactical Training Group, Pacific, courses available at https://www.ttgp.navy.mil; Tactical Training Group, Atlantic, courses available at https://www.csg4.usff.navy.mil/ttgl; Expeditionary Warfare Training Group, Pacific, courses available at https://www.ewtgpac.navy.mil; Expeditionary Warfare Training Group, Atlantic, courses available at https://www.csg4.usff.navy.mil/ewtglant; Joint Targeting School, courses available at https://www.jcs.mil/Doctrine/Joint-Training/Joint-Functional-Schools/JTS; CYBERCOM, https://www.cybercom.mil; Surface and Mine Warfare Development Center courses available at https://www.surfpac.navy.mil/nsmwdc; Naval Aviation Warfare Development Center courses available at https://www.airpac.navy.mil/Organization/Naval-Aviation-Warfighting-Development-Center; Naval Information Warfighting Development Center courses available at https://www.navifor.usff.navy.mil/Organization/Operational-Forces/NIWDC.

MODERN DAY MARINE®

WALTER E. WASHINGTON CONVENTION CENTER, WASHINGTON D.C.

APRIL 30 - MAY 2, 2024

REGISTRATION IS OPEN

350+ Exhibiting Companies, OBJ 1 Wargaming Convention, Briefings from Senior Leaders and DoD Personnel, the Latest Warfighting Innovations, and More.

Scan the QR Code for More Information

MARINE CORPS LEAGUE — SEMPER FIDELIS

MARINE CORPS ASSOCIATION — EST 1913

Modern Day Marine is not open to the public. All registrants must provide proof of identity with a Government issued photographic ID and must demonstrate that they have an "identifiable relationship" with the Marine Corps.

The Department of Defense, the Department of the Navy, or U.S. Marine Corps does not endorse any company, sponsor or their products or services

Educate to Win

Preparing Marines for victory in the next war

by Maj Timothy Warren

In the early hours of the next large conflict, it will be the Marines on the ground who will buy time for the generals and admirals to orientate to the operational picture and begin the decision-making process. Those Marines will be the first eyes and ears in complex scenarios and their ability to make informed decisions will reverberate throughout the operational and strategic levels. As such, it is imperative that we educate our Marines from day one on how to observe, think critically, and make educated decisions as much as we train them how to be strong, fast, and accurate. It will not be enough for our aircraft mechanics, logisticians, and infantry to only think about their jobs. Those Marines need to be educated enough to know how their roles will affect grand plans and how to derive alternate means to achieve *the why* even if they are prevented from accomplishing the standard technicalities of their MOSs. Officers can provide their commander's intent all day, but if their troops are not trained to think critically, then that intent is all but useless. Leaders today need to enable their Marines to draw upon ample educational resources so that the Marine Corps will be the fiercest and most intelligent fighting force in the world tomorrow.

>See bio on page 52.

Buying Time with Education

The preparations that most organizations make for conflict rarely are adequate for actual hostilities, resulting in initially high losses of time, resources, and manpower. Even in the best organizations, it takes time for leaders to make the organizational and strategic changes that are required to conduct more effective campaigns during chaotic periods. These leaders can be gifted more crucial time for analysis and reorientation if their troops at the tactical level are making educated decisions that slow down and frustrate the enemy—even if only by minutes or hours. This concept has played out countless times from the opening days of World War II where on the ingenuity of the Marine defenders on Wake Island diverted critical Japanese resources,[1] to the Battle of the Bulge where fireteam-sized pockets of soldiers frustrated the German advance,[2] and to Iraq where the highly skilled troops in the cities gave the generals time develop the successful surge strategy.[3] All these scenarios, and so many more, clearly demonstrate where critical decision making at the tactical level created operational and strategic maneuver space for hard-pressed commanders.

If war with the People's Republic of China happens, the Marine Corps in the Pacific will likely find itself outnumbered and stretched thin, with a small chance that anyone will accurately predict the time and location of the opening salvos.[4] This environment is why we must educate Marines today and train them to think bigger than their individual jobs. The young Marines manning fighting positions and airfields need to have been trained tactically and educated formally in such a way that they can face a myriad of unknown situations and make decisions that will gain military and political ground which will help achieve operational and strategic goals. This is not to say that a platoon of tactically sound doctors of philosophy and engineering majors is going to prevail against a technical over-match or an enemy with superior positioning. But, with the complexity of modern warfare, the Marine Corps can ill afford not to have highly educated

Wargaming, both tabletop and computer-based, are powerful tools to reinforce planning and decision-making skills in professional military education. *(Photo by PFC Samuel Ellis.)*

troops forward deployed, especially with the ample opportunities available.

The Marines today are smarter than at any time in the past, but so are our adversaries.[5] It is imperative for every leader in the Marine Corps to personally seek out more education for themselves and encourage their troops to go above and beyond required professional military education (PME), MarineNet courses, and the Commandant's Professional Reading List. Noncommissioned officers and junior officers need to carve out time from busy workloads and workups to allow their Marines the maneuver space to expand their knowledge and cognitive abilities. Staff noncommissioned officers and senior officers need to make additional education a requirement for those same noncommissioned officers and junior officers. There is no reason why a sergeant on his third deployment or working twelve-hour shifts, six days a week is earning a degree while other Marines are working standard hours and just biding time until they rotate.[6] Leadership needs to be engaged to ensure that every Marine's mental capacity is being expanded as rigorously as their physical capacity is.

Professional Military Education

The Marine Corps should also reexamine how it requires and delivers PME—especially for its officers. There is significant value in the Marine Corps PME program, ensuring that Marines of similar grades have a base knowledge of staff skills and operational planning, but the nearly zero-sum game of being PME complete for the next promotion should have more latitude. It makes little sense for an infantry officer with sufficient time in line companies, on staffs, and with a Master of International Relations to be passed over for not having their PME complete. It makes even less sense to have a limited duty officer with an exceptional resume and bachelor's and master's engineering degrees devote even more of their precious time to learning materials that may not make them a better officer in their field. By no means should the Marine Corps scrap the PME program, but there should be better means for determining if a Marine should have a level of PME waived or be given a much-reduced version of a PME program. There may simply be cases where more educated and experienced people are being pushed to the side because they didn't conform to the organization's educational norms.

The Marine Corps needs the bulk of its personnel synchronized in its warfighting methods to ensure that it can deliver proper mass at the point of attack at the correct time, and this is where PME comes into play. However, the Marine Corps also needs a cadre of Marines who have achieved academic success outside of the Service's approved programs to ensure fresh ideas are cultivated. Is the institution really harmed if that cadre does not have one level of PME in a few cases? If a Marine wishes to pursue a program on their own and they have the requisite professional experience, then the institution should allow them a pass on PME and embrace their cognitive growth. BGen Forrest Poole said it best when he encouraged the 2023–2024 Commandant's Fellows and Marine Corps War College students to change the way that they think, to take electives on subjects they know nothing about, because the Marine Corps needs them to think differently to win the next war.[7]

The push for a fully educated force, whether it be through PME or civilian education has proven time and time again to be a game changer for the Marine Corps.[8] At any given time, the Marine Corps has about one-third of its complement in a school and it pulls a large percentage of its officers out of the fleet completely for a year (or more) of further education.[9] This education has paid dividends for the Marine Corps from its officers drawing on their Army[10] and Navy War College[11] lessons in World War I,[12] to Marines in World War II using automotive mechanical skills to conduct hasty aircraft repair,[13] up to enlisted Marines using engineering,[14] law enforcement, medical, and many other types of learned civilian skills in Iraq and Afghanistan to enhance stabilization operations.[15] The question is then, if education is of known value, how do we get the other two-thirds of the Marine Corps to continue their education while also carrying out their primary assignments?

Educational Options

This article would never argue that any Marine should neglect their primary assignments for additional education. However, if all levels of leadership embraced educating the full force, time could be found without cutting into a Marine's performance or their liberty. Universities such as American Military University and Troy University (just two examples of many) have short semesters, flexible class schedules, and only charge tuition assistance while offering a wide array of traditional courses.[16] Embry-Riddle Aeronautical University Worldwide and Sonoran Desert Institute have similar setups while offering unique degrees in aeronautics (maintenance, airfield management, metrology, etc.) and firearms science (gunsmithing and ballistics); knowledge that could be useful for Marines who must deal with unforeseen scenarios in future operations.[17] These civilian universities have designed many of their programs so that service members can further their educations in a moderately paced fashion and within normal fiscal means. Another option for a minimally intrusive educational experience is Sophia Learning. This organization charges 99 dollars per month and offers over 50 college courses that students can complete at their own pace.[18] Sophia Learning provides the students with all the materials and course requirements while leaving the rest to the student's discretion and timeline. When the student has gotten as far as they want to go with Sophia Learning, their credits transfer to any number of civilian colleges for degree completion. With these options, there is little reason why leaders could not encourage and assist their Marines in furthering their education.

U.S. Naval Community College and the Air University's Online Master's Program are two free options for Marines to achieve a higher level of education while also staying in the professional education realm. The U.S. Naval Community College was developed in partnership with several civilian univer-

sities to allow enlisted service members a flexible means to achieve an associate degree. The degrees that this unique organization offers cover areas such as nuclear science, cyber, leadership, aviation maintenance, and logistics while also providing an impressive curriculum of professional naval education.[19] The credits earned here are also transferable so that enlisted service members can go on to achieve their bachelor's at other institutions if they so wish. The Air University's Online Master Program offers senior O-3 and O-4 officers the option of earning a Master of Military Operational Art and Science with concentrations in nuclear weapons, leadership, or operational warfare while also earning credits for traditional professional military education and joint professional military education phase 1. This program is highly challenging while offering a delivery method comparable to Marine Corps University distance education programs and other civilian universities.[20] Taking that program before or after Marine Corps Command and Staff College gives officers unique views into how each branch views the same level of warfighting and presents officers with new ways of approaching problem sets. Both, the U.S. Naval Community College and the Air University's Online Master's Program will ensure that our fleet Marines have access to free, flexible, and highly valuable educations while they continue to learn their primary jobs and conduct operations.

A final means of using education to ensure that the Marine Corps is prepared for the next conflict is with SkillBridge. This program allows service members to be granted up to 180 days of permissive duty to focus solely on training full-time with approved industry partners. Many see this as a program to just thank service members for their dedication by allowing them to have a fully paid internship for the final months of their contract.[21] Whereas some commands may see this as a burden since the Marine's billet is left empty until their actual end of active service date, neither perspective articulates three critical warfighting effects that SkillBridge provides.

The most direct benefit of SkillBridge is to allow the Marine several dedicated months to learn a new skill set on the military's dime and time. Many, if not most, of these service members will transition to Inactive Ready Reserve or the Retired Reserves. In case of a large war, it will be these reservists with their newly acquired civilian skills who will bolster the active ranks. The second way SkillBridge will support future combat operations is through recruiting. These Marines who get to participate in SkillBridge will have a great opportunity granted them during their final active months. This opportunity will likely leave a positive view of their time in service while also helping them to be successful in the civilian world. These successful veterans will reflect positively on the Marine Corps and will be seen by potential recruits who may desire to emulate their success. Additionally, successful veterans with a positive view of the Marine Corps may suggest enlistment to quality citizens they encounter in civilian life. The final means by which this program will help gain battlefield success is through morale. Young Marines will see the Marines before them be rewarded for their service with a fully funded internship of their choosing. This will demonstrate to the young Marines that their leadership and the Marine Corps appreciate the stress that they had gone through over their contract. A Marine who knows their work is appreciated is more likely to work harder, train better, and fight tougher. SkillBridge is not a drain in a unit's staffing goal; rather, it is an investment into the Marine Corps fighting ability in the future.

Conclusion

Education alone will not win the next war. The Marine Corps needs people who are physically fit, disciplined, and highly trained in their primary fields and in basic Marine skills. However, the same Marines are likely to be dispersed and partially isolated in the opening stages of any war with the People's Republic of China. We need as many of these Marines to be educated and able to think of solutions to problems as they appear with only their wits and the resources at hand. The Marine Corps spirit and highly educated Marines will buy time for the Joint Force to enact the plans that will lead the Nation to success in any conflict.

Just imagine a small unit of Marines assigned to defend and operate a remote forward arming and refueling point airfield in the first island chain. You may have a Marine who has studied the dicey cultural history between the United States and the islands' native population, another who has a degree in airfield operations, another with a gunsmithing degree, a reservist who is a fully experienced engineer, and several with working knowledge of partner services communication styles and cultures. This unit could accomplish amazing feats with just the knowledge and skills that their Marines bring to the table. The potential is endless for what the Corps could accomplish if most of its Marines were educated with the vast opportunities available to them while on active duty if only encouraged and provided the opportunities to do so. This effort just takes buy-in from the leaders of those Marines.

Notes

1. Charles River Editors, *The Battle of Wake Island: The History of the Japanese Invasion Launched in Conjunction with the Attack on Pearl Harbor* (Scotts Valley: CreateSpace Independent Publishing Platform, 2016).

2. John Toland, *Battle: The Story of the Bulge* (Lincoln: University of Nebraska Press, 2016).

3. Thomas E. Ricks, *The Generals: American Military Command from World War II to Today* (New York: Penguin, 2013).

4. MGen Mullen, reported by Diana Stancy Correll, "A Culture of learning: Why the Marine Corps Is Promoting Education, Training in Its New Doctrine," *Marine Corps Times,* May 2020, https://www.marinecorpstimes.com/news/your-marine-corps/2020/05/19/a-culture-of-learning-why-the-marine-corps-is-promoting-education-training-in-its-new-doctrine.

5. Gen Robert B. Neller, *Statement on the Posture of the United States Marine Corps. Delivered to the Congressional Defense Committees of the 115th United States Congress*, April 2018.

6. Based on the personal experiences of Maj Timothy Warren.

7. Discussion between BGen Forrest Poole and FY23–24 Commandant of the Marine Corps Fellows and Marine Corps War College students on July 27, 2023.

8. Staff, "The History of the Marine Corps University," *Marine Corps University,* n.d., https://www.usmcu.edu/About-MCU/History-of-MCU.

9. Gen Eric Smith, "Proceedings Podcast EP, 346: Marine General Eric Smith on Manpower, Training, and Education." *Proceedings Podcast*, Podcast audio, July 10, 2023, https://www.usni.org/magazines/proceedings/the-proceedings-podcast/proceedings-podcast-ep-346-marine-general-eric-smith.

10. Staff, *Rosters of Army War College student graduates, 1904–1940* (Carlisle Barracks: U.S. Army War College, Historical Section, 1958).

11. Staff, *Register of Officers: 1884–1977* (Newport: The United States Naval War College, 1977).

12. George B. Clark, *A List of Officers of the 4th Marine Brigade* (N/A: The Brass Hat, 1995).

13. Charles River Editors, *The Battle of Wake Island: The History of the Japanese Invasion Launched in Conjunction with the Attack on Pearl Harbor* (Scotts Valley: CreateSpace Independent Publishing Platform, 2016).

14. Cpl Ken Melton, "Reserve Marine's Civilian Skills Improve Living Conditions for Fellow Marines," *Marines.mil,* May 23, 2005, https://www.2ndmardiv.marines.mil/News/Article/Article/514690/reserve-marines-civilian-skills-improve-living-conditions-for-fellow-marines.

15. LtCol Melissa D. Mihocko. *U.S. Marines in Iraq, 2003 Combat Service Support During Operation Iraqi Freedom,* (Washington, DC: History Division, United States Marine Corps, 2011).

16. Information available at https://www.amu.apus.edu; and https://www.troy.edu/military-veterans/marines/index.html.

17. Information available at https://worldwide.erau.edu/administration/military-veterans; and https://www.sdi.edu/military/active-duty.

18. Information available at https://www.sophia.org.

19. Information available at https://www.usncc.edu/s/about.

20. Information available at https://www.airuniversity.af.edu/GCPME/OLMP.

21. Information available at https://skillbridge.osd.mil/program-overview.htm.

Khalkin Gol War

Expeditionary operations in remote locations

by Mr. Joseph Miranda

A common situation in warfare is conducting expeditionary operations in regions beyond regular logistical support. This situation is covered in Decision Games Khalkin Gol War in World at War issue #95.

The historical background for the game goes back to the summer of 1939 when the Soviet Union and Japanese Empire were technically at peace. In May, there was a clash between their respective forces at the Khalkin Gol River on the ill-defined border between Japanese-occupied Manchuria and Soviet-dominated Outer Mongolia.

The bigger picture was that the Japanese were fighting an undeclared war with the Republic of China. Moscow sided with the Chinese largely to maintain the balance of power in East Asia and saw the clash at Khalkin Gol as a chance to gain a victory that would give the Japanese second thoughts about moving into Mongolia.

At this time, Manchuria (or Manchukuo as the Japanese termed it, meaning empire of Manchuria) was a major possession of Tokyo and the base for the Japanese Kwantung Army whose leaders had their own policy, which included further expansion toward Inner Asia. (Incidentally, the Japanese referred to the fighting here as an incident to avoid the international diplomatic implications of declaring war.)

In any event, the clash at Khalkin Gol escalated into a series of moderately sized battles as both sides reinforced the frontier: the Japanese with more Kwantung units as well as Manchukuoan and Inner Mongolian forces, the Soviets with their Far East Red Army and Outer Mongolian formations.

>Mr. Miranda is a prolific board wargame designer as well as being the past editor of both Strategy & Tactics and Modern War magazines. His designs include a wide range of topics from the classical era to the near future and have covered combined-arms, low-intensity conflict, and hybrid operations. He is a former Army Officer and has conducted numerous professional seminars on modeling and simulation. Mr. Miranda has also authored several Decision Games special interest publications to include an upcoming issue on the First Indochina War.

The fighting around Khalkin Gol continued over the summer—with neither side gaining an immediate decision (and is also known as the Battle of Nomonhan after a nearby village). The Soviet Red Army had superior numbers of light tanks and armored cars. The Japanese Army Air Force had the edge in the skies, while their Army infantry possessed superior tactical skills.

Providing additional difficulties was the logistical situation. Both the Soviet and Japanese armies were operating at the end of extreme lines of communications. The main battlefield lacked rail connections back to friendly bases, while the road net was inadequate—to say the least.

Finally, the Kremlin placed Gen Georgy Zhukov in charge of the Khalkin Gol front. Zhukov carefully built up his logistical system, employing truck convoys to move men and supplies forward while the Red Air Force challenged the Japanese in the skies. On 20 August 1939, Zhukov launched a corps-sized mechanized assault, exploiting the maneuverability and shock effect of Red Army tanks. The Japanese, commanded by Gen Michitaro Komatsubura, fought hard but could not deal with the Soviet armor. In mid-September, the Japanese high command in Tokyo agreed to a ceasefire, and the Khalkin Gol Incident was resolved with a border change in favor of Moscow.

Nonetheless, there were officers within the Kwantung command who wanted to continue the fight, moving up reinforcements to Khalkin Gol from other parts of Manchukuo in an attempt to gain a victory on the far Mongolian frontier. Their proposal was flatly turned down by Tokyo, but what if they had gotten their way and the Khalkin Gol incident had turned into a full-scale war? That is the topic of the game which models campaigning in a remote theater of operations.

Campaign on the Steppes

The *Khalkin Gol* game map shows the military geography of the theater of operations including western Outer Mongolia, Manchukuo, Menjiang (Japanese-controlled Inner Mongolia), and bordering regions of the Soviet Union to the north. Most of the terrain is wide open steppe or desert, with intervening marshes. Some ranges of hills and low mountains run along the periphery, making for a sort of arena. Several small rivers bisect the map.

Communications are via a network of roads and trails (the term roads is used rather loosely here, these being mainly

improved tracks). There is a rail line running from Manchukuo to the Soviet Union but none in the Mongolias where most of the fighting will take place. Control of roads is important because this enhances ground unit mobility. It also makes possession of junctions vital as a way to switch forces laterally.

There is an unbuilt railroad following a course from the Soviet town of Borzya (on a spur of the Trans-Siberian Railroad) to Tamsag Bulak in Outer Mongolia near Nomonhan. The Soviets can build this railroad in the course of a scenario by expending supply. While this construction can take the course of the campaign, it pays off in the long run by providing the ability for the Red Army to rapidly move its units and supply forward. Soviet victory in battle hinges on the buildup of theater infrastructure.

Logistics are a major part of the game. Players can mobilize supply units which they can then use to support operations. The game uses a multi-impulse sequence of play. Normally, each unit can move and attack only once per turn. But if the player expends supply, units within a logistical radius can take a second impulse during the turn. If you set up your logistics properly, your forces can conduct sweeping maneuvers and big breakthroughs. This requires planning a turn ahead to get supply units into position and get back to controlling lines of communications.

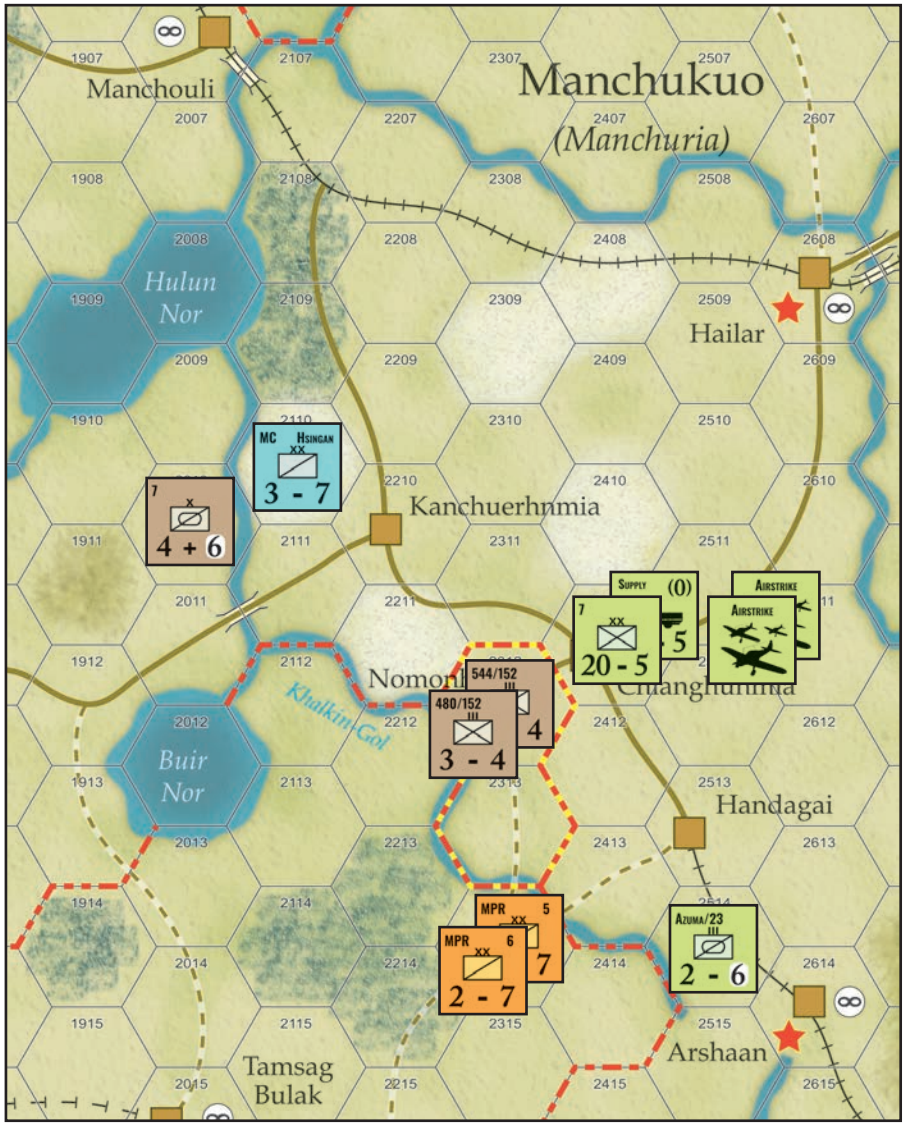
Aerodromes are on the map (the circled infinity symbols). These are vital because they are used to base air units which can then fly missions. It is here where the Japanese have an edge because their air units have longer ranges than their Soviet foes. The range factor takes into account both aircraft fuel capacity and doctrinal factors. The Japanese were trained up for long-range operations whereas the Red Air Force at this time was oriented toward close support missions. (This is a way to place both material and non-material factors into a single game function.)

There are three air missions: air superiority (to attack enemy air units in aerodromes), ground attack (to attack enemy ground units, especially enemy supply units), and close air support (to enhance friendly combat forces engaged with the enemy). Airstrikes are vital because they are a way to project combat power forward in areas where it can be otherwise difficult for ground units to operate. The vertical dimension overcomes groundbased limitations. The Japanese also have an air supply group that can provide logistics support to units that would be otherwise cut off by outrunning their lines of communications.

There is no interception of incoming airstrikes owing to a lack of air warning systems and operating in a pre-radar environment. Thus, airpower is mainly an instrument of offensive warfare. This gets back to the game strategy. Ground forces seize aerodromes to move air units forward and then conduct airstrikes to enhance further offensive operations.

The game map also shows major objectives (red stars), largely towns important for military and political

Japanese assault on Nomonhan. Japanese 7th Division (green units) makes a frontal attack on Nomonhan village which is held by two Soviet regiments (brown units). Japanese are supported by a supply unit (which can be expended to provide an attack bonus) and two airstrikes based on the Hailar aerodrome. Soviet north flank is secured by a mechanized cavalry brigade and their south flank by Inner Mongolian cavalry (orange units). Japanese north flank is secured by Manchukuoan cavalry (blue) and the south by an armored cavalry regiment.



reasons. The village of Nomonhan is a major objective because it was a center for the border conflict which led to the Khalkin Gol campaign in the first place. Other objectives include towns that were logistical and transportation centers (such as the aforementioned Tamsag Bulak). Essentially, players are fighting to gain a dominant position in the theater which can then be translated into a later negotiated settlement on your side's terms.

There are other ways to project power. One is by unconventional warfare. Players can dispatch agents and attempt to convert them into partisans that are useful for operating in the enemy rear area. The agent and partisan units are named after various intelligence organizations and fronts that participated in the original campaign. It is all part of joint operations in a campaign on a far frontier of the emerging Second World War.

Zhukov builds a railroad. Japanese vanguard has advanced westwards out of range of its groundbased supply system. The Japanese air supply group provides support to the armored cavalry regiment. Meanwhile, Gen Zhukov has used the Far East Military District engineers to push the Soviet railroad as far as Bain Tuman which serves as the forward supply point. The main Soviet jumping-off point is the town of Borzya across the border in the Soviet Union. There, a Red Army tank brigade and another supply unit prepare to rail up to the front. The Red Army armored train provides security against Japanese-controlled Menjiang partisans (green unit) attempting to cut Soviet lines of communications.

KHALKIN-GOL WAR is an operational-level, two-player wargame covering a "what if" Japanese-Soviet war in Mongolia in 1939. The historical campaign saw a series of limited actions in the late spring and early summer of 1939 along the Khalka River (Khalkin Gol) on the Manchukuoan/Outer Mongolian border. The campaign ended in a corps-level battle in August 1939 in which the Soviets decisively defeated the Japanese and produced a cease-fire between the two antagonists. The assumption of the game is that both Tokyo and Moscow decided instead to turn this into a full-scale war.

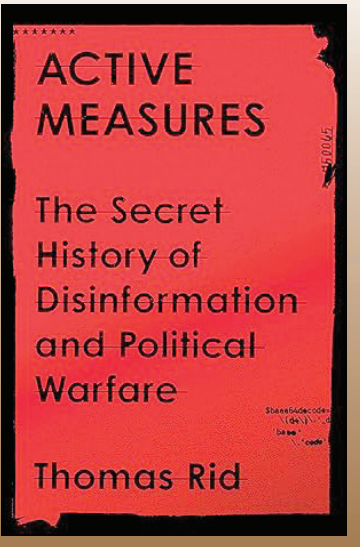
Each turn of play represents a month of operations. Each hex on the map is approximately 30 kilometers across. Ground units are mostly built around divisions, with breakdowns into brigades and regiments. Air units represent anything from an elite squadron to a mediocre group.

D-Day at Saipan is a solitaire game that simulates the first five days (15 to 19 June 1944) of the US invasion and conquest of the island of Saipan. Despite heavy resistance, over 8,000 Marines of the 2nd and 4th Marine Divisions managed to reach the shore that first morning and by the end of the day approximately 20,000 men had established a beachhead, despite having suffered over 2,000 casualties. Over the next five days the Marines were joined by the Army's 27th Infantry Division and began pushing inland toward Aslito Airfield and Japanese forces in the southern and central parts of the island. Conquest of the island provided a secure base that put the Japanese home islands within range of B-29 bombers.

ORDER ONLINE: decisiongames.com/wpsite/mcaf
Bulk orders please call 661-679-6821

Active Measures

reviewed by Capt Ayesha Ahmad



ACTIVE MEASURES: The Secret History of Disinformation and Political Warfare. By Thomas Rid. New York, NY: Profile Books, 2020.
ISBN: 9780374718657, 488 pp.

Thomas Rid's 2020 released book is a rare combination of an interesting spy adventure and standard history textbook. Rid uniquely interweaves large historical events with the stories of individuals, agencies, governments, and leaders. As a leading expert in the field of information technology conflict, Rid reinforces the importance of understanding the information environment as it continues to influence strategic decisions. *Active Measures: The Secret History of Disinformation and Political Warfare* can serve as the foundation for understanding today's dynamic operational environment and is therefore worth a read for all Marines.

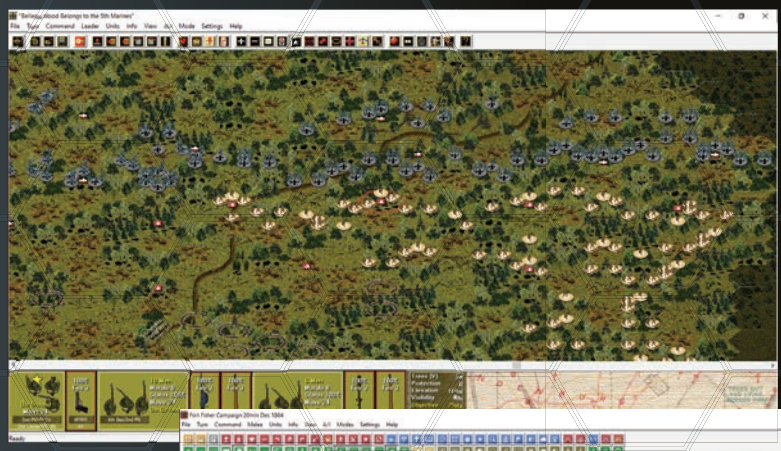
Thomas Rid begins his work with a quick introduction to the nature of information and influence. He then defines for the reader the purpose of disinformation as "exacerbation [e] existing tensions and contradictions within the adversary's body politic, by leveraging fact, fakes, and ideally a disorienting mix of both." While simultaneously providing three distinctive elements to define active measures, "[active measures] are not spontaneous lies by politicians, but the methodical output of large bureaucracies ... contain an element of disinformation ... is always directed toward an end, usually to weaken the target adversary," Rid subsequently sections the book into historical periods covering 1921–2017. In each section, Rid illustrates the political environment of the time, detailing both the physical and emotional nature of the people and their leaders. He then weaves in the active measure tactics used by opposing and friendly governments, analyzing each one's flaws and successes. Rid concludes his book with a relevant and current analysis of truth, its nature, and its relations to both an individual and society, ultimately providing one answer to the philosophical question: what is truth?

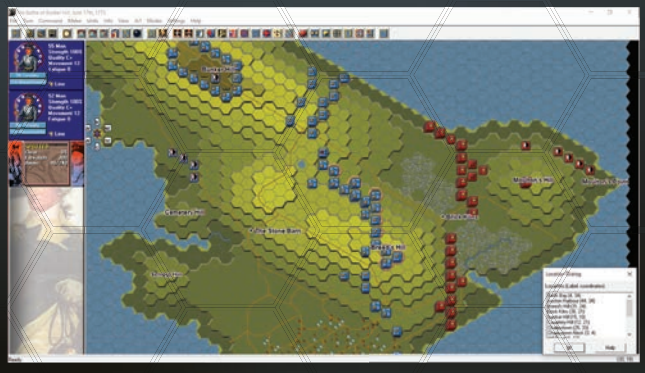
>Capt Ahmad is an Air Support Control Officer deployed in support of JTF MATTHEW with the 24 MEU, commanded Air Support Company, Marine Air Support Squadron 1, and is a qualified Weapons and Tactics Instructor. She is currently a candidate for MS in Information Warfare Systems Engineering from the Naval Postgraduate School.

The world is evolving at a rapid rate due to technological advances in information sharing. It is therefore critical every professional warfighter has a basic understanding of the current information environment and its modern history. *MCDP 1* suggests that the nature of warfare does not change; rather, the means of warfare evolve with human advances. In the Digital Age, information—and its propagation—has become a weapon. It is with that recognition the Marine Corps updated its doctrine to add information as the seventh warfighting function with MCBULL 5400—published in 2019. This addition indicates the information domain is critical to current and future engagements. Its integration and understanding by all must therefore be on par with fires and sustainment. Like in many endeavors to gain a complete understanding, history provides the most obvious starting point. *Active Measures* is the place to start. It provides a unique lens to view the last century by linking political objectives with tactical employment strategies. It provides a foundational understanding through historical examples of disinformation tactics and insight into the philosophical question of what truth is. Other suggested readings on this topic includes *Hoodwinking Hitler* by William B. Breuer and Rid's full published works.

Active Measures ... provides a unique lens to view the last century by linking political objectives with tactical employment strategies.

USMC





Wargame Design Studio Discounts Available to All MCA Members

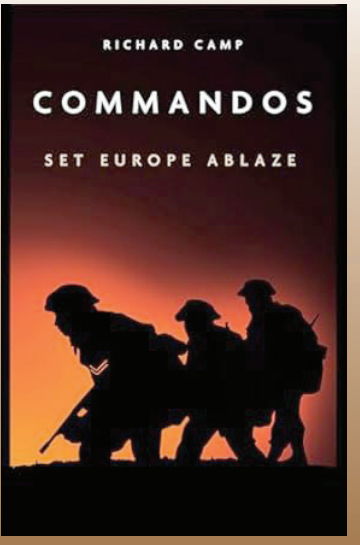
Receive a **25% discount** on all Wargame Design Studio games available through MCA Extra Rations

Fight in an array of conflicts from the Musket and Pike Era to the present day

For additional information, check out the Wargame Design Studio Website: wargameds.com

Commandos

reviewed by MajGen Ted Hopgood



COMMANDOS: Set Europe Ablaze. By Richard D. Camp. Philadelphia, PA: Casemate 2021.
ISBN: 978-1636240084, 237 pp.

The exciting and riveting actions of this outstanding book are told in a remarkably clear and inspiring fashion!

The author, Col Camp, spent his 26-year active duty career either training for combat or actually leading men in battle. He knows well of what he writes as he spent his career at or near the tip of the spear. His portrayal of the unique personalities and skills that combine to make an elite fighting force are both clear and entertaining. Each well-described training evolution is graphically described and will stimulate either memories or awe, usually both! An example of the realism that bleeds from every page is the hand-to-hand combat instructor, Maj William Fairbairn. This instructor, who developed the Fairbairn-Sykes Commando Dagger which is still in use today, teaches either win the fight or die.

In June 1942, two U.S. Marines were ordered to detach from the 1st Raider Battalion and report to the British Army for commando training. Capt Jim Cain and GySgt Leland Montgomery, along with a soon-to-be-reduced group of British soldiers, are welcomed to the commandos with a "little stroll." The seven-mile forced march from their arriving train stop to their new home, the Commando Basic Training Center at Achnacarry, located in the rugged highlands of Northwest Scotland, is an attention-getter as well as an accurate pacesetter for the unrelenting training and combat action that rapidly ensue.

The traditional and never-to-be-forgotten introductory greeting, which gains immediate control over the trainees, will ring true to every former recruit and officer candidate. "By the time you complete training, you will belong to the finest troops in this war, the commandos. When the time comes for you to face the Hun and he sees the determined glint in your eyes and the cold steel of your bayonet, he'll drop his rifle and run like the hounds of hell are after him!" This brief but pointed "welcome aboard" is delivered by the 6-foot-6 Commando colour sergeant who greets the new trainees from behind his beautifully waxed handlebar mustache, extending inches on either side of his mouth. Readers will observe Colour Sergeant Angus Bourne throughout this compelling story. Bourne is the epitome of British military excellence, and as his aspiring commandos will soon learn, he is "as tough as woodpecker lips!"

The delivery of pithy instruction and the exchange of humorous dialogue between all the trainees and their rock-hard training staff make this book so much more entertaining than just a bland after-action report. Of course, our two U.S. Marines are quick to give out as much guff as they receive! Never to be out-done, outshot, or out-marched, the skipper (Capt Cain) and the gunny (GySgt Montgomery) quickly join their new mates in their competitive and demanding training evolutions. The all-out effort and combat skills required from the commando trainees are expertly explained by the author with fast-moving accuracy.

Colour Sergeant Bourne not only leads the trainees, now designated as Commando 62, but he also joins it! Never at a loss for words or giving sound advice, his guidance, delivered daily, will soon prove its worth on the big line. "After seven weeks when we leave here, you will be exceptionally skilled killers. Our training includes small arms explosives, field craft, map-reading, field problems, and physical exercise." The commando school standard is a seven-mile march with packs and rifles in one hour.

>MajGen Hopgood is a retired Marine Corps Officer.

An example of the realism that bleeds from every page is the hand-to-hand combat instructor, Maj William Fairbairn. This instructor ... teaches either win the fight or die.

YOUR #1 SOURCE FOR MILITARY REFERENCE

SMARTbooks

SMARTbooks: Reference Essentials for the Instruments of National Power (D-I-M-E: Diplomatic, Informational, Military, Economic).

SMARTbooks can be used as quick reference guides during operations, as study guides at education and professional development courses, and as lesson plans and checklists in support of training.

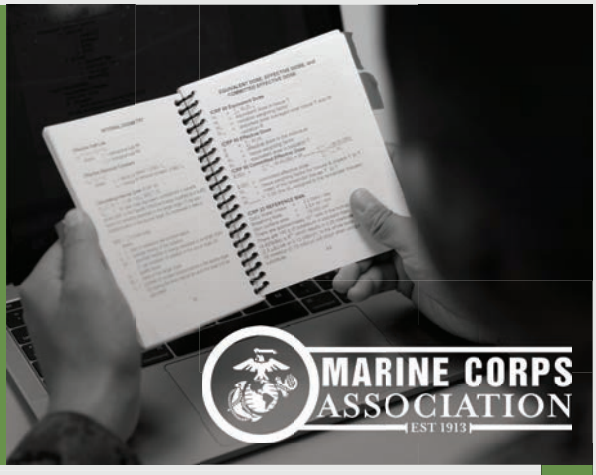
Recognized as the doctrinal reference standard by military professionals around the world.

WHAT IS A SMARTbook?

MCA IS HERE TO HELP

MCA members will receive **10% off their purchases** from The Lightning Press SMARTbooks website. Use code **SMART-MCA-10** for your order.

The MCA will also work with any unit or school on funding discounted bulk order of 50 or more copies. Call the MCA Foundation at **(866) 622-1775** or email **mca@mca-marines.org** for more information.



GET YOUR EDGE. ORDER TODAY.

Web: www.TheLightningPress.com
Email: SMARTbooks@TheLightningPress.com
24-hour Order & Customer Service: 1-800-997-8827
Mobile: 863-409-8084

SMARTbooks

The Lightning Press
INTELLECTUAL FUEL FOR THE MILITARY

No safety nets are used to ease the challenges of the Tarzan Course (ropes and trees) or when abseiling (rappelling down a cliff). As team morale builds and the difficulty of training increases, trainees who might have a liability, such as fear of height, are slowly coached through the requirement but then must complete the challenge at full speed. Commando training is not pass/fail. It is "pass" fully or report back to your unit. There are no participation medals.

A live-fire training raid near the end of their seven-week instruction cycle is interrupted with orders to return to base. A real mission, critical to the war effort, is assigned to 62 Commando. A fourteen-man commando raiding party, with Capt Cain in the lead boat and GySgt Montgomery and Colour Sergeant Bourne in the second craft, is assigned to land on a Channel Island occupied by a German FREYA surveillance radar station. The commandos are ordered to destroy the radar site, capture a radar operator, and bring back key radar components.

The execution of this demanding and dangerous raid is exceptionally well-described by Camp. The close-quarter fighting is not without friendly casualties. Readers will feel like they are members of the raiding party and experience the fear and excitement of close, personal combat. Part IV of this captivating story is the harrowing return of the now bloodied 62 Commando to its launch point at the Portsmouth Naval Base. With torpedoes and direct fire delivered by the thoroughly aroused German Naval forces landing amongst the boats carrying the Commando 62 team, the author describes the perilous nighttime ocean battle with non-stop, every-page excitement.

This book has it all! Readers will sweat through difficult training, experience vivid and heroic combat, and even smile over a bit of mild romance for the skipper. Enhancing the genuine feel of this expertly crafted book are cameo appearances by both Churchill and Lord Mountbatten. And, to further pique interest, Loreena McNeal, a captivating Scottish Lassie, and Capt Cain, the dashing Yank, share a mutual attraction but the war keeps them separated, or does it? Nonetheless and fortunately, Loreena is assigned to the Cabinet War Room in London where she becomes privy (as is the reader) to the commando raid and its uncertain outcome!

USMC

In Like a Lion · Out Like a Lamb

Welcome to Spring at THE MARINE SHOP!

UA Womens Tech Baseball Tee Flawless
$39.99

UA Tech Short Sleeve Tee
$44.99

UA Freedom EGA Tee
$34.99

Marines Red Hat
$24.99

USMC Khaki Hat
$24.99

Vintage USMC Cap
$19.95

USMC Garden Flag
$15.99

"The Few The Proud" Garden Flag
$14.95

USMC Car Flag
$12.95

Shop today at Marineshop.net or call us at (703) 640-7195

Follow us on social media! @themarineshoponline @TheMarineShop1

The MARINE Shop
SERVING MARINES AROUND THE WORLD

Index to Advertisers

Marine Corps Gazette

Upcoming 2024 Monthly Themes

June Edition
Author drafts due: NLT March 20, 2024

July Edition
Author drafts due: NLT April 17, 2024

August Edition
Author drafts due: NLT May 15, 2024

September Edition
Author drafts due: NLT June 20, 2024

October Edition
Theme: MCISRE
Author drafts due: NLT July 17, 2024

Editorial Policy

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. Material submitted for publication is accepted or rejected based on the assessment of the Editor-in Chief. The *Gazette* provides a platform for fact-based discussion and welcomes both content written by Marines as part of their official duties and content written independently by Marines and the public. Professional ethics, copyright law and ease of reading demand that writers provide the sources of direct quotations and paraphrases. Assertions of fact that are not common knowledge and cannot be easily checked must be supported with a verifiable source.

The Board of Governors of the Marine Corps Association has given the authority to approve manuscripts for publication to the Editor-in-Chief. The Editorial Advisory Panel judges all *Gazette* writing contests. Editorial Advisory Panel members are listed on the *Gazette*'s masthead in each issue. The panel represents a cross section of Marines by occupational specialty, professional experience, age, rank, and gender. A simple majority rules in its decisions. Corrections and retractions can be published on the *Gazette* webpage within two working days and normally appear in the next available print edition of the magazine.

Writers' Guidelines

The *Gazette* welcomes material in the following categories:

- **Commentary on Published Material:** The best commentary can be made on the *Gazette*'s LinkedIn® page.
- **Letters to the Editor:** Limit to 300 words or less and DOUBLE SPACED. Email submissions to gazette@mca-marines.org. 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.
- **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 and evidence presented to support logical conclusions. In the case of articles that criticize, constructive suggestions are sought. Footnotes are required for direct quotations, and paraphrasing. Use the Chicago Manual of Style for all footnotes and citations. A list of all source materials used is required, to include bibliography, journal articles, and interviews.
- **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. However, we will do our best to publish your article as soon as possible, and the *Gazette* staff will contact you once your article is slated. If you prefer to have your article published online, please let us know upon its acceptance.

Submissions: Email articles as an attachment to gazette@mca-marines.org. Save in Microsoft Word format, DOUBLE SPACED, Times New Roman font, 12 point. Photographs and illustrations must be in the public domain or the author's original work. Specify the source. In the case of copyrighted images, proof of permission/license to use must be provided by the author. The Defense Visual Information Distribution Service (DVIDS) and unit/installation combat camera sections are the best sources of public domain photographs. Photographs must be in high resolution native files TIFF, JPEG, or PNG format (300 dpi) 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.) One sentence captions are welcome. Include the author's full name, mailing address, telephone number, and email addresses—both military and commercial if available. Any queries may be directed to the editorial staff by calling (703) 640–0180.

Skydio

Ensure readiness with Skydio AI-powered drones

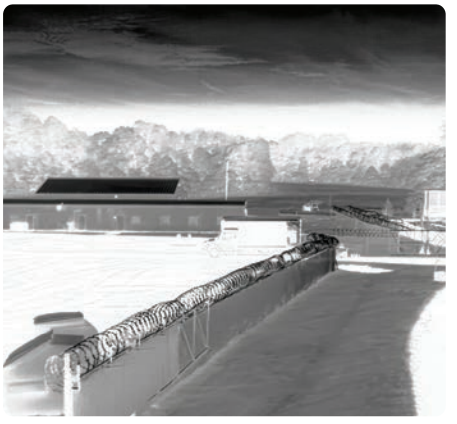
It takes every member of the Marine Corps, working together, to deter and win conflict. With world-leading artificial intelligence capabilities, Skydio drones are force multipliers that create effective human-machine teams across the Corps.

Generating tactical advantages downrange

See the enemy first. Skydio drones deliver organic and real-time intelligence, surveillance, and reconnaissance (ISR), empowering field units and command staff with actionable insights. Navigating complex environments autonomously, these small, uncrewed aerial systems (sUAS) generate asymmetric situational awareness advantages with minimal cognitive load for operators.

Ensuring ship and aircraft readiness

Maintain asset health. Skydio drones streamline the inspection of ships and assets, reaching areas that are otherwise inaccessible or hazardous. With high-resolution imaging and 3D modeling capabilities, drones identify potential issues before they become operational setbacks, ensuring that the Marine Corps remains battle-ready at all times.



Protecting personnel at bases and installations

Secure your perimeter. Skydio drones bolster base security by providing continuous surveillance and rapid response capabilities. Autonomous patrols detect threats with both visual and thermal cameras, without putting personnel at risk, creating a security posture that deters adversaries and protects Marines.

The future operating environment is now.

Agility, efficiency, and readiness are critical.

Skydio is standing by to serve you.

Learn more at skydio.com/solutions/defense

PERSISTENT SYSTEMS

NETWORKING THE BATTLEFIELD

An all-domain multi-mission TRL 9 solution approved for use on USMC networks

NETWORKING THE IOT IN AIR, ON LAND, & AT SEA

MAGTF AND JADC2 INTEROPERABILITY

PERSISTENTSYSTEMS.COM