Advancing Cyberspace Operations

Opportunties to Leverage MARSOC and MARFORCYBER

by Maj Tyler Bahn

The Marine Corps is well-positioned to lead DOD integration of operations in cyberspace, sea, air, and land domains as the country cycles out of armed conflict, back to sub-threshold competition and preparation for conflict.[1] To do so, it needs to embrace an integrated Marine Special Operations Command (MARSOC) and Marine Forces Cyber Command (MARFORCYBER).

>Maj Bahn is the Commanding Officer, Marine Special Operations Company India, 2D Marine Raider Battalion, Marine Corps Forces Special Operations Command.

The Current Situation

The United States has aggressively decreased its counter-violent extremist organization efforts around the world while pursuing great power competition. The shift from counter-violent extremist organization (C-VEO) to competition reduces military tactical interactions with enemy and allies alike. Special Operation Forces' (SOF) enduring forward presence now accounts for an even higher proportion of global awareness through partnerships, surveillance, and advising.

Simultaneously, the Marine Corps is marching toward the Expeditionary Advanced Base Operations (EABO) construct with significant medium- and long-term acquisitions to support the evolution. However, worrisome fiscal constraints present a very real challenge to modernization, capability development, acquisition, and readiness. The dynamic implores partnerships and prudent use of existing modernization efforts, especially those that help offset the Marine Corps financial load.

These events are not occurring in a vacuum. As Simon Sinek discussed during the MARFORCYBER-led Irregular Warfare Symposium and in his book, *The Infinite Game*, the United States is engaged in an infinite game, which has known and unknown players who can enter and leave at any time based on their willingness, desire, and resources. David Kilcullen pointed out in his lecture, "Future War: Sub-threshold Campaigning in an era of Great Power Competition," that the line between state and non-state adversary capabilities and tactics is becoming less defined. Non-state actors like VEOs have access to capabilities previously only held by state actors, whereas state actors are using VEO tactics to carry out their objectives in the increasingly connected world. Our competitors are effectively using their instruments of national power in unison and exploiting seams that constrain the United States.

Joint Publication 3-12 describes cyberspace as three interconnected layers: physical network layer, logical network layer, and cyber-persona layer. These layers represent vectors for attack and requirements for defense. Consider the ransomware attacks against Colonial Pipeline and hundreds of others, compromised SolarWinds code, and Russian social media bots as examples.[2] However, cyberspace operations (CO) are complex. They are neither easy nor a guaranteed win. Jason Crabtree wrote in his 21 June 2021 Foreign Policy Argument that, despite the constant discussion of cyber warfare in today's military discussions, CO did not play a significant role in the 2020 conflict between Armenia and Azerbaijan over the Nagorno-Karabakh region. Hacks against state officials, shutting down websites, limiting internet access, and active social media efforts failed to significantly degrade either side's fighting capabilities.

Success in cross domain cyberspace operations generally requires spotting, assessing, and accessing targets; cyber operators and associated capabilities; post-operation analysis and assessments; and stakeholder engagement. Spotting, assessing, and accessing targets are best accomplished by those with persistent access to a given domain: Cyber Operations Forces (COF) in cyberspace and cyber-sensitized SOF in physical domains. COF and their tools generally reside at U.S. Cyber Command (USCYBERCOM) for coordination and management. While analysis and assessments in cyberspace often falls to COF, there are opportunities to spread the considerable burden amongst other units seeking integration. Finally, appropriately engaging the vast stakeholder networks for most integrated operations requires a group effort.

Consider a hypothetical example: MARSOC is deploying a Marine

Special Operations Team (MSOT) to Country X. MARFORCYBER wants to conduct offensive CO against proxy actors in that country. The MSOT currently deployed to Country X notifies MARFORCYBER that they have identified a new vector for operations against the enemy. MARFORCYBER views the vector as vulnerable, so they begin developing a plan to affect the enemy. The deployed MSOT begins planning and coordination with their host nation partners and the U.S. Embassy in Country X while the next MSOT to rotate sends a team to MARFORCYBER Headquarters, where they develop a concept to be tested during the upcoming MARSOC Company Collective Exercise. The new MSOT then deploys, executes the mission with MARFORCYBER, while the recently redeployed MSOT conducts an out brief with MARFORCYBER to identify any missed opportunities. Finally, a third MSOT would shape its members' individual skills training for mission specific enhancements. Throughout this process, the MARSOC Cyber Cell maintains continuity for CO as teams rotate and the MARFORCYBER Littoral Operations Cyber Cell (LOCC) integrates MEU planning for expanded effects.

Eventually, aggressive actions by the proxy force towards local embassies cross the threshold of armed conflict and the MEU moves to the country. MARFORCYBER can provide additional short-term fulfillment of SOF requests for CO support but cannot dedicate analysts to the problem permanently. If properly prepared, the MEU can support the fast rise in required analytic assessment work necessary for continued SOF and MEU CO as the MEU begins developing additional accesses with similarly equipped reconnaissance forces.

The Marine Corps' *Tentative Manual for EABO* in paragraph 5.7.3 notes:

> Special operations force [SOF] integration provides vital means to conduct Operations in the Information Environment (OIE), especially in cooperation and competition. SOF's unique authorities, relationships, and capabilities provide access and placement to conduct OIE across all functions and capability areas to meet commander's intent. OIE often provide the critical means to compete below the threshold of armed conflict. They also enable and set conditions for EABO and littoral force priorities and lines of effort. SOF increasingly employ OIE to shape the environment to seize and sustain advantage in competition and enable naval expeditionary forces to win in conflict.

In a world where the threat of violent extremism remains, the focus on great power competition grows, and the line between the two blurs, it is essential that the Marine Corps embraces its most connected, engaged, and technologically advanced forces. A deliberate, habitual relationship allows MARSOC and MARFORCYBER to lead DOD innovation while raising the FMF's competitive capabilities through numerous existing touchpoints between the two Marine Forces (MARFOR).

MARSOC and MARFORCYBER Background

MARSOC and MARFORCYBER are strikingly similar. In those similarities lie significant opportunities. MARSOC units, under combatant control of USSOCOM, and MARFORCYBER units, under combatant control of USCYBERCOM, have access to funds and equipment from both the Marine Corps and their combatant command.

Since inception, a plurality of both organizations' forces has been persistently engaged in operations against the Nation's enemies. Each is heavily invested in international and interagency partnerships at the tactical level. Both organizations require highly skilled, mature, high-demand individuals to rise to the challenges of the future operating environment—individuals that the FMF are hesitant to lose. Though many of these forces' successes are shrouded in secrecy, MARSOC and MARFORCYBER are routinely praised by the commands they support for their outsized success despite each being the smallest component contributions to the component commands (COCOM) to whom they belong.[3]

The MARSOC mission is to recruit, train, sustain, and deploy scalable, expeditionary forces worldwide to accomplish special operations missions assigned by U.S. Special Operations Command (USSOCOM).[4] To accomplish that, [they] equip and train Marines to succeed in austere conditions against a wide range of adversaries.[5]

MARFORCYBER's mission is to conduct full spectrum CO—to include operating and defending the Marine Corps Enterprise Network, conducting defensive CO within the Marine Corps Enterprise Network and Joint Force networks, and when directed, conducting offensive CO in support of joint and coalition forces—in order to enable freedom of action across all warfighting domains and deny the same to adversaries. USCYBERCOM has further tasked, "The Marine Corps [as] the service that supports SOCOM."[6] While other Service cyber components undoubtedly integrate with USSOCOM forces, MARFORCYBER is charged with maintaining dedicated integration mechanisms on behalf of USCYBERCOM, including their Cyber Operations-Integrated Planning Elements (CO-IPE) collocated at USSOCOM Headquarters.

Since inception, a plurality of both organizations' forces has been persistently engaged in operations against the Nation's enemies.

MARSOC and MARFORCYBER: A Beneficial Relationship

The most significant value that MARSOC and MARFORCYBER provide to the Marine Corps, USSOCOM, and USCYBERCOM is created when MARFORCYBER and MARSOC are

MARSOC and MARFORCYBER have many similarities that could create to synergies in operations employment. ***(Photo by Cpl Ethan Green.)***

closely integrated. Just as the FMF performs specific, critical national defense tasks, MARSOC and MARFORCYBER have specific, resource intensive missions assigned by their COCOMs. However, they can be used to fill Marine Corps multi-domain gaps while improving their execution of COCOM directed missions.

While the FMF will work with all service cyber and SOF components, the author's time at MARFORCYBER unequivocally affirmed that Marine Corps recruit training instilled in MARFORCYBER Marines an unparalleled appreciation for the person on the ground. The common Marine Corps ethos allows MARSOC, MARFORCYBER, and the MEU to integrate quicker and better than with other cyber and SOF components.

Some may contend the FMF would be better served having closer relationships with each of the forces, separately. Certainly, a well-connected Marine Corps is a better Marine Corps, but competing interests demand prioritization of resources. This article maintains that mission and command relationships between the MARSOC and MARFORCYBER allows more efficient advancement of competitive effects for the entire Marine Corps. Furthermore, USCYBERCOM is aligned to COCOMs, not Services, in support of the role as cyber coordinating authority. MARFORCYBER support to USSOCOM, as directed by USCYBERCOM, provides a structured pathway for communications between MARSOC and MARFORCYBER via shared planning conferences, liaisons, and the CO-IPE throughout USSOCOM.

The Marine Corps can invest in a close MARSOC-MARFORCYBER team by increasing lines of communication, manpower efficiencies, investing in relevant training and infrastructure, and defining equipment testing and training relationships. The Marine Corps can codify exactly how it benefits from the two MARFORs by establishing formal agreements with USSOCOM and USCYBERCOM to stabilize expectations. CO is not a magic bullet for competition and future conflict. However, enabling tactical commanders in all domains to layer effects through investments in education, infrastructure, and relationships will allow the U.S. military to better compete in the newest domain.

Opportunity 1: Create More Pathways for Knowledge Exchange

Effective CO is hard. Timing, stakeholders, capabilities, and the enemy situations open and close windows of opportunities at random. As such, it is critical to maintain closely integrated networks of cyber units to identify and act on opportunities as quickly as possible. Increasing the lines of communication between MARFORCYBER LOCC elements, Theater Special Operations Commands (TSOC) CO-IPEs, the MARSOC Cyber Cell, and MEU cyber sections can help identify opportunities and even posture forces to act on fleeting opportunities.

MARSOC and MARFORCYBER can benefit from integrating MARSOC Cyber Marines into the MARFORCYBER formation for temporary rotational periods. Those MARSOC Cyber Marines will gain MOS credibility from USCYBERCOM exposure, while adding capacity to MARFORCYBER's ability to support USSOCOM. If those Marines nest within the MARFORCYBER LOCC, MARFORCYBER, MEU, and MARSOC, cyber entities will be collocated to create long-term operational impacts. The enhanced and direct flow of information will contribute to a "trifecta" of information flow between MARSOC, MARFORCYBER, and the MEU via the LOCC.

The Marine Corps can also support pipelines that push intelligence, cyber, and information operations Marines to gain experience in MARSOC and MARFORCYBER. Early MARFORCYBER experience is critical for 17XXs to learn their trade, but tactically minded Cyber Marines can be transferred to MARSOC to quickly apply their craft. The heavily joint, combined USSOCOM and USCYBERCOM commands provides opportunities for Marines to integrate with interagency and international partners. In turn, the more senior, capable Cyber Marines will be experienced enough to "sit at the table" to drive cyber integration in the MEUs.

Opportunity 2: Allow MARSOC to increase its networks and "Inkblot"

MARSOC's greatest contribution to CO is its persistently forward deployed presence and influence. Enabling access to key physical layer cyber terrain by expanding MARSOC's areas of influence as much as possible through partners, networks, and relationships with regional stakeholders increases CO's effectiveness.

Operations in cyberspace are often not "one shot, one kill." New concepts face an uphill battle for approval where multiple, diverse stakeholders must be convinced, and acceptable opportunities must be identified. A MARSOC and MARFORCYBER combined network enables spotting, assessing, developing, coordinating, troubleshooting, and amplifying opportunities in cyberspace that support FMF options. For MARSOC to accomplish this, it must allocate manpower to engage key stakeholders in embassies and interagency headquarters, embed planners at TSOCs, and send elements to developing crisis areas in addition to existing combat zones. For example, MARFORCYBER CO-IPEs and MARSOC liaison officers engage operational leadership and TSOCs; MARSOC Special Operations Forces Liaison Elements engage country teams; MSOTs engage host nations and partner forces forward; and MARFORCYBER engages the interagency and cyber partners from the National Capital Region.

Training ranges can be designed to replicate the electromagnetic spectrum of towns to support multi-domain awareness at the lowest levels …

MARSOC may use efficiencies in manpower gained from non-CSOs and SOOs filling key staff roles at battalion, regiment, and component levels, allowing raiders to fill more roles in TSOCs. Better placement at TSOCs will allow raiders to identify more opportunities and influence decisions relevant to joint CO. Seeking deployed billets in U.S. Embassies abroad, such as Special Operations Forces Liaison Elements, enables access to the country teams who can support or stall MARFORCYBER efforts. Finally, smaller decentralized MARSOC formations could help offset its relatively small size and increase its role as a connector for units like MARFORCYBER.

Opportunity 3: Pre-deployment Training and Coordination

One of the great benefits of COs is that a force can create effects on the battlefield without being on the battlefield. The application for specially trained *Mission Impossible*-style hackers manipulating code from a forward position is limited. Instead, the goal should be to enable the MARSOC "inkblot" of influence to characterize the information environment, identify potential targets, and know how to communicate opportunities to the community of interest or request appropriate support for integrated operations.

MARSOC and MEU intelligence analysts must also be cross trained to incorporate USCYBERCOM analytical tools into their own collections. Better training and access to key systems will help increase self-sufficiency of forward units and help limit the scope of requested support. Many analytic training opportunities already exist but are not regularly shared with ground force analysts.

Until the DOD's understanding of cross-domain warfighting is better codified, courses benefit from bringing multiple organizations together. The resulting networks are critical to maintaining awareness of which units are willing and able to act on key opportunities. Ideally, integrated training will lead to better pre-deployment integration between MARFORCYBER, MARSOC, and the MEU. Specific planning with the three entities can determine where and what type of cyber accesses are likely to support MEU plans, enabling advanced preparation. MEUs can request early support through USSOCOM and USCYBERCOM to prepare for upcoming MEUs or anticipated contingencies while MARSOC seeks the operational agility to move forces to fill MEU-specific—temporary OIE requirements as required by the supported COCOM. The MARFORCYBER LOCC is uniquely positioned to conduct such meetings.

Education should be reinforced with training. Readiness exercises at the Army's National Training Center and Joint Readiness Training Center incorporate USSOCOM units into each rotation and Army Cyber units have been involved in training since 2017.[7] Given the small sizes of MARSOC and MARFORCYBER, they cannot dedicate support to each training evolution. Instead, the Marine Corps could choose certain rotations to act as full spectrum integrated training with incorporation of Marine Special Operations Companies and MARFORCYBER COF. The exercise forces could cycle through real world deconfliction issues and conduct proofs concepts prior to deployments.

Opportunity 4: Invest in Critical Infrastructure

Training and increased demand for communication with the MARFORs and interagency requires investment in the infrastructure required to support them. Current training ranges provide excellent opportunities for integrating crew served weapons and indirect fires but few are purpose-built to integrate CO with the ground scheme of maneuver. Until ranges are upgraded, mobile training suites designed to help coordinate cyber fires and maneuver as well as contracted support are available, though with varying relevance to a real-world scenario. Training ranges can be designed to replicate the electromagnetic spectrum of towns to support multi-domain awareness at the lowest levels while purposefully enabling joint training with COF.

Perhaps most importantly, tactical leaders need to have direct communications with their interagency counterparts by increasing access to Sensitive Compartmented Information Facilities on bases, at forward deployed locations, and on the MEU. Decentralized execution of multi-domain operations can be better enabled by empowering subordinate leaders with access to information and communication with interagency partners. The cost benefit analysis of increasing access to key systems is beyond the scope of this paper but hobbling the nation's forward sensors by limiting access is no doubt an opportunity cost.

The MEU is limited in its ability to move into a COCOM, identify relevant targets in cyberspace and develop and execute multi-domain CO by the time it leaves. More than likely, SOF is already on the ground, has better access, and possesses better understanding of the local dynamics. If the MEU moves to support a specific operation short of armed conflict, it is still limited. However, in the example at the beginning of the article, a MEU is excellently positioned to add critical analysis and assessment capability to support what would be a growing number of CO requirements if properly equipped with ample network access, Sensitive Compartmented Information Facilities space, and analysts trained on USCYBERCOM analytic programs in preparation for MEU operations. Given the MEU occupies Navy ships, this would likely be a joint effort with joint benefits.

Opportunity 5: MARSOC Integration with Marine Corps Testing, Evaluation, and Fielding

In his guidance, the Commandant of the Marine Corps supports the USMC being "Fast Followers" in Artificial Intelligence, Machine Learning, and Data Science.[8] A close MARSOC-MARFORCYBER team can keep the Marine Corps pulse on integrating OIE with maneuver units across USSOCOM and USCYBERCOM, and quickly feed it back to the FMF. Beyond using USSOCOM and USCYBERCOM resources and units for capability development, SOCOM can leverage partners and the local economy to fulfill force projection gaps. For OIE, a close MARSOC-MARFORCYBER relationship allows development of cheap alternatives, place fillers, and force multiplying capabilities in advance of and in support of a turnover to the MEU.

Pragmatically, the Marine Corps stands to save money by leaning on MARSOC and MARFORCYBER access to USSOCOM and USCYBERCOM resources for experimentation. As each component develops new equipment for OIE, USSOCOM and USCYBERCOM act as a funnel for all the disparate ideas being developed. The Marine Corps should not miss the opportunity to systematically integrate these efforts using these two MARFORs.

Adversarial state and non-state actors are rapidly iterating tactics and equipment in the battlefield. Meanwhile, U.S. forces are losing access to battlefield laboratories to test innovations most notably in Afghanistan, Iraq, and Somalia.[9] USCYBERCOM and USSOCOM enemy engagement allows quicker battlefield refinement. MARSOC is best suited amongst MARFORs to create or borrow other USSOCOM SOF/Cyber ideas, test in realistic training events, and field against the enemy.

Closing

MARSOC's enterprise agility, MARFORCYBER's tasking and experience supporting USSOCOM, and their common identity as amphibious warfighters positions the Marine Corps to synergize multi-domain operations during competition and preparation for armed conflict. MARSOC and MARFORCYBER should not be directly aligned to support the Marine Corps by their COCOMs, but the Marine Corps stands to gain significant multi-domain capability if it nurtures a connected MARSOC and MARFORCYBER. These concepts are not new, but they must be exercised to move cyber integration from a buzz phrase to an effective warfighting instrument.

Notes

[1] Headquarters Marine Corps, *MCDP 1-4, Competition*, (Washington, DC: 2020).

[2] William Turton and Kartikay Mehrotra, "Hackers Breached Colonial Pipeline Using Compromised Password," *Bloomberg*, (June 2021), available at https://www.bloomberg.com; Reuters and Christopher Bing, "White House Blames Russian Spy Agency SVR for SolarWinds Hack," *Reuters*, (April 2021), available at https://www.reuters.com; and Lulu Garcia-Navarro and Eric Westervelt, "How Russia Weaponized Social Media With 'Social Bots,'" *NPR*, (November 2017), available at https://www.npr.org.

[3] Gen Richard Clarke, "MARSOC Change of Command Speech," (speech, MARSOC Change of Command Ceremony, Tampa, FL, June 2020); and U.S. Senate, *USCYBERCOM Commanding General Paul Nakasone, Statement before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities*, (Washington, DC: March 2020).

[4] Special operations missions include civil affairs, counterinsurgency, counterterrorism, countering weapons of mass destruction, direct action, foreign humanitarian assistance, foreign internal defense, hostage rescue and recovery, military information support operations, security force assistance, special reconnaissance, unconventional warfare, and preparation of the environment. See Staff, "About USSOCOM," United States Special Operations Command, (n.d.), available at https://www.socom.mil.

[5] Staff, "Marine Forces Special Operations Command," MARSOC, (n.d.), available at https://www.marsoc.marines.mil.

[6] *USCYBERCOM Commanding General Paul Nakasone, Statement before the House Committee on Armed Services Subcommittee on Intelligence and Emerging Threats and Capabilities.*

[7] Staff, "Combat Training Center Rotations Continue to Drive Evolution of Army Cyber-Electromagnetic Activities," U.S. Army, (June 2017), available at https://www.army.mil.

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

[9] Michael D. Shear and Jim Tankersley, "Biden Defends Afghan Pullout and Declares an End to Nation-Building," *New York Times*, (August 2021), available at https://www.nytimes.com; Staff, "US Combat Forces to Leave Iraq by End of Year," *BBC*, (July 2021), available at https://www.bbc.com; and Brian W. Everstine, "After Leaving Somalia, U.S. Troops Now 'Commuting to Work' From Other Nations," *Air Force Magazine*, (April 2021), available at https://www.airforcemag.com.

UB MC