Hacking the Minds of Decision Makers

Preparing strategic corporals for future warfare

by Capt Corey A. Ware

>Capt Ware is a 1702 Cyberspace Warfare Officer currently assigned as a Cyberspace Warfare Instructor at Marine Detachment Fort Gordon. Previously, Capt Ware served 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. He also served as the JTF-ARES Liaison Officer to CJTF-OIR, collaborating directly with the USCENTCOM Joint Cyber Center, USCENTCOM Cyberspace Operations-Integrated Planning Element, JFHQ-Cyber Army, and all components planning cyberspace operations within Iraq and Syria. Capt Ware also served as one of two cyberspace warfare officers attending resident EWS during the 2022 academic year.

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, the capability area of cyber dominates the media as the new buzzword across the military and private sector. Many experts strive to understand it; however, it is something everyone in the digital age interacts with and consumes every day. The ability to develop unorthodox solutions to complex problems is a hallmark of cyberspace professionals. Rather than relying solely on history, deployment experience, or wargames where solutions and outcomes are publicly known, cyberspace professionals encounter problems that cannot be read about in open source due to classification. Placidly, the mindset of a cyberspace 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.[2] As such, creative minds drawing ideas from both fiction and non-fiction can have a significant impact on mission success.[3] In an age of competition, the DOD anticipates operating in a contested information environment. The Marine Corps must send more experienced cyberspace 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 cyberspace operations into all levels of war.[4]

Faculty and students at Marine Corps professional military education (PME) do not possess the requisite knowledge or experience to educate the force on cyberspace operations.[5] Since the creation of the Marine Corps' 17XX cyberspace MOS in 2018, there is a limited population of retained Marines and experienced personnel outside of Marine Corps Forces Cyberspace Command (MARFORCYBER).[6] Even fewer are assigned as instructors or students to formal schools outside of primary MOS training.[7] Meanwhile, "competitors deterred from engaging the United States and our allies in an armed conflict are using cyberspace operations to steal our technology, disrupt our government and commerce, challenge our democratic processes, and threaten our critical infrastructure."[8] As the DOD engages in great power competition, MAGTFs "are currently unable to effectively operate in cyberspace because of a limited number of cyber 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."[9] Furthermore, Marines are not exposed to cyber request processes or planning considerations during PME. Due to a lack of education on cyberspace operations, future decision makers and strategic corporals remain unable to make justified decisions involving cyber or understand how to request effects from a cyberspace capability.

Training also does not resemble potential cyberspace effects U.S. forces will encounter against near-peer adversaries. 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, and Iran. 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 on 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."[10] Cyberspace attacks could also degrade or destroy com-

mand 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.[11] 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 into the full spectrum of military operations."[12] 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 servicemembers to serve as "the most conspicuous symbol of American foreign policy."[13] 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."[14] Failure to conduct training with problems that service members may face in the cyber 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.[15]

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 cyberspace operations with the combatant commander and MAGTF requirements. First, the Marine Corps must increase the 17XX faculty and student population at PME. The *Commandant's Planning Guidance* describes PME as "student-centered learning using a problem-posing methodology where our students/trainees are challenged with problems that they tackle as groups in order to learn by doing and also from each other."[16] Lessons learned from a diverse conference group or staff during seminars, lectures, curriculum development, or wargames are intangible, especially when including personnel with different experiences from new communities like cyber, information operations, and space. Increasing cyber 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 U.S. Cyber Command.[17] By creating a planning environment that normalizes "asking for authorities to use tools in new domains" or other diplomatic, informational, military, and economic instruments of power, future planners can maximize the ability to incorporate non-lethal cyber fires into all levels of war.[18] 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 cyberspace operations]."[19] Cultivating cyber enlightenment across the Marine Corps begins with formal education supplemented with training.

Secondly, assigning subject matter experts to key billets within the Combatant Command Cyberspace Operations-Integrated Planning Elements (CO-IPEs) and the MEF Information Groups (MIGs) and will assist with training and professionalizing the force about cyberspace operations. "CO-IPEs are organized from USCYBERCOM" personnel generally from each Joint Force Headquarters-Cyber (JFHQ-C) service component "and are co-located with each CCMD for full integration into their staffs."[20] (Provided figure from JP 3-12 should be displayed here). As such, the CO-IPEs provide direct liaison authority/reach back to U.S. 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

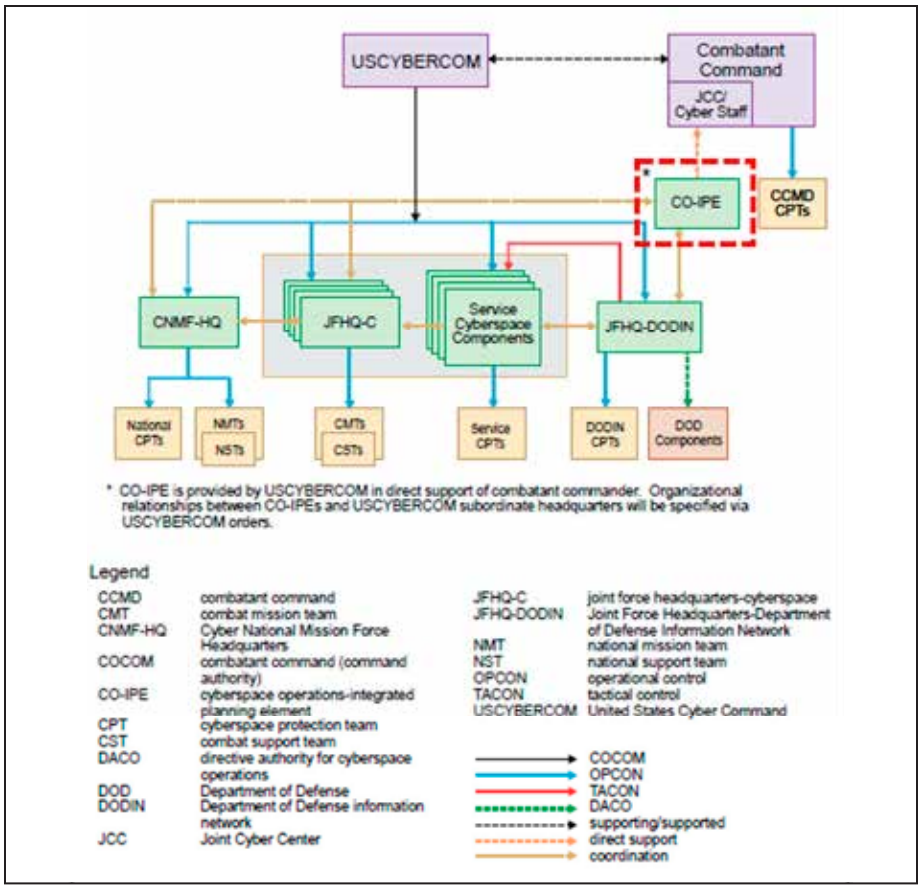

Figure 1. Routine Cyberspace Command and Control. 1702 majors and/or 1710/1720 chief warrant officers as well as 1799 master sergeants/master gunnery sergeants should be embedded in certain or all CCMD COIPEs, who are also co-located with CCMD staffs. ***(Figure provide by the author from Figure IV-1,*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

personnel to bolster cyberspace planning initiatives and concepts.[21]

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 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 is not acclimated to this capability area.[22] Furthermore, operational effects in cyberspace do not necessarily lead to servicemembers being physically endangered on the battlefield. By conditioning decision makers with non-lethal options, this awareness will boost their confidence in approving cyberspace concept of operations. The addition of 17XX cyberspace Marines to CCMD CO-IPEs will spawn serendipitous value to CCMD staffs by capitalizing on the Marines' understanding of Amphibious Ready Group/MEU (Special Operations Capable) employment in the Marine Corps planning process and ability to advance cyberspace opportunities by leveraging integration between Marine Special Operations Command and MARFORCYBER.[23]

Gen Berger, 38th Commandant of the Marine Corps, and then-MajGen Mathew G. Glavy, Commander of Marine Corps Forces Cyberspace Command and Joint Task Force Ares, discuss current and future offensive and defensive cyber operations. LtGen Glavy is now Deputy Commandant for Information. ***(Photo by SSgt Jacob D. Osborne.)***

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.[24] Key lessons learned from after-action reports and pre-deployment training have shown an appreciation for this new domain based on information operations synchronized with cyber injects.[25] 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.[26] 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 information 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, 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. "The rest of the Marine Corps ... [must] start learning the ways of cyber," and appointing experienced personnel to key billets to train and advise decision makers and planners will reinforce the integration of cyber into military operations.[27]

Sending personnel with experience from MARFORCYBER ... will enable the MIGs to design similar exercise networks that can effectively train the operating forces at all echelons of command.

A counterargument claims decisive actions against a near-peer adversary will involve physical maneuver using expeditionary advanced based operations; 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 both the deception of the adversary's sensors and a common operational picture, utilizing non-lethal means, to enable effective fire and maneuver.[28] Transitioning from a generation of counterinsurgency operations, Gen Berger has made it clear the Marine Corps must embrace its amphibi-

ous roots and immerse the FMF into understanding the Navy's composite warfare concept, which recognizes Marine Corps integration.[29] Marines on keyboards will not be crucial to mission success on the battlefield; priority of efforts should address only the MEU 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," therefore, incorporating information-related capabilities into education and training should be secondary.[30]

Irrevocably, cyberspace operations will continue to dominate current and future warfare. In planning rooms of the operating forces to 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."[31] 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 cyberspace 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.[32]

Notes

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

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

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

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

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

6. Daniel J. O'Donohue, *MARADMIN 136/18 Establishment of the Cyberspace 1700 Occupational Field (OccFld)*, (Washington, DC: March 2018).

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

8. Department of Defense, *Summary Department of Defense Cyber Strategy 2018*, (Washington, DC: 2018).

9. Austin Duncan, "On Cyber," *Marine Corps Gazette* 102, no. 4 (2018).

10. 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).

11. 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).

12. James N. Mattis, *Summary of the 2018 National Defense Strategy of The United States of America*, (Washington, DC: Department of Defense, 2018).

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

14. Ibid.

15. *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).

16. *38th Commandant's Planning Guidance.*

17. 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).

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

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

20. Joint Chiefs of Staff, *Joint Publication 3-12, Cyberspace Operations*, (Washington, DC: June 2018).

21. Information available at https://www2.manpower.usmc.mil/ncp/rankMos;mos=1702;mosType=P.

22. *38th Commandant's Planning Guidance.*

23. 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.

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

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

26. 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.

27. "Leading Cyber Marines with Maj. Gen. Matthew G. Glavy."

28. *38th Commandant's Planning Guidance.*

29. Ibid.

30. Ibid.

31. 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.

32. *MCDP 1-4*, *Competing.*