Ducere

Lead to the new front lines

by Maj Lawrance P. Andrus, Jr.

>Maj Andrus served as the Executive Officer for 2d Marine Raider Battalion in 2019 and as the Signal Center Director for Special Operations Task Force-North Iraq in 2020. He is currently serving as the Communications Officer for the Marine Raider Training Center in Camp Lejeune, NC.

Since Marine Forces Special Operations Command is behind the cyber revolution kill chain, Marine Corps Forces Special Operations Command (MARSOC) should replace the existing command and control (C2) structure to adapt to rising alternatives to non-kinetic operations. Cyber is a growing concern for the U.S. national strategy. However, the need for cyberspace planning does not fit well with the current approach to planning from tactical leaders, C2 force structure, and sustainable talent management. MARSOC can adapt quickly by adjusting internal controls, tactics, and procedures without the need for external influence. Additionally, altered habits of action and habits of thought will drive the "lead" that operators need for the next war with a great power.

The first step needed to adapt and regain the cyberspace initiative is to plan for it explicitly. Mission analysis briefs need to focus on analyzing cyberspace. The critical flaw is that tactical-level planners tend focus only on the enemy and its kinetic and non-kinetic effects—more specifically, effects of information operations. Tactical planners do not plan for nor do they account for cyberspace during planning. This oversight is equivalent to World War I generals failing to account for and quickly adapting to the lethality of the machine gun. The difference is that the effects of the cyber domain are invisible and often occur beyond the tour of the planners. The solution requires the explicit requirement to plan for the cyberspace area of operations, including blue cyberspace, red cyberspace, and gray cyberspace. This first step will set conditions for proper support requirements that require leveraging within the MARSOC command. Next, a structure must exist within MARSOC to best align with the operational needs of the tactical planner.

MARSOC capabilities to operate in any domain must include cyberspace operations. (Photo by LCpl Zachary Ford.)

The Marine Special Operations Company and Team (MSOC) must receive a fire capabilities report of cyber assets within the area of operation. Like artillery, the fire capabilities report will include what fire capabilities are available to the tactical leaders. Rather than advocate for authorities at the team level to conduct cyberspace operations, the team must have the ability to request fires within their area of operations (AO). For this to work, the cyber planners within MARSOC must be employed to liaison with the Battalion, Component, and external Cyber National Teams, and it must not hamper with traditional bureaucratic C2 structure a means to do so. The MSOC will need fundamental information: What are the capabilities, what effects will it provide, and how to request? Answering these questions will rely on the structure of MARSOC and how it must revolutionize its approach to such technical and dispersed capabilities and authorities. MARSOC requires a dedicated primary cyberspace staff officer dedicated to the MARSOC staff. The cyberspace officer will advise the commanding general, advocate for capabilities, and design the required C2 support structure to meet the needs of the MSOC at the tactical level. In other words, the establishment of the

"Cyber Reach Back" structure and for the MSOCs to have direct knowledge of the cyber kill chain.

Lastly, the final step is to utilize existing commercial off-the-shelf certifications that directly instruct on hacker tactics, techniques, and procedures. MARSOC should consider cyber funding threat-based training or offensive security such as Certified Ethical Hacker or Offensive Security Certified Professional. The idea is that incidental cyber warriors are not restricted to a limited amount of military occupational specialties but as a supplement too. These levels of certifications will ensure that cyber is no longer synonymous with information operations and will alter the habit of thought with regards to cyber options at the tactical level. The tactics, techniques, and procedures in the cyber realm are too complicated to brief to the entire population; however, take the knowledge of an incidental cyber warrior and combine that with the operational need of a commander; the result will be new requirements that will leverage existing abilities within the department of defense. Those new requirements will propel MARSOC by increasing the cyber tempo and climb to the modern cyber revolution age.

Below is an example of how cyber operations can enable a tactical level leader:

Before the assault, team leaders receive direct intelligence that dark web chat rooms indicate that an impending action by U.S. forces is imminent. The leader was already aware that the enemy collected intel from compromised commercial-off-the-shelf (COTS) systems that partners were utilizing, thus eliminating COTS equipment for the operation. The leader decides to combine Information and Cyber Operations before any physical assault. Information operations commence convincing the population that the local enemy force intends to shut down power and electricity to deter U.S. forces from entering the city. Next, since the leader is already aware that the U.S. Cyber National Teams have embedded logic bombs within the peer nation's infrastructure, he decides to execute the preapproved cyber fires on the water and power infrastructure; power and electricity are now offline. No power and no water mean no cellular coverage and no access to the internet. Now water limits the ability of enemy forces to sustain themselves without a resupply. The leader assesses the effects of the information environment. This example is how cyber can influence shaping operations.

Below is a limited list of example tactics, techniques, and procedures:

- Intel can leverage the FBI: Intel collected from the dark web, chat forums and compiled by an LNO that can feed the decision-making cycle of a deploying unit.
- Realtime indicator of compromise that will directly affect the grey space within an AO. Examples include COTS assets such as remote advise and assist assets and "smart" devices.
- Integrate DOD blue space and conventional intelligence and cyber intelligence.

The examples illustrate a simplistic view of what enhanced cyber operations can accomplish for the tactical level leader. What is more important for the long-term agility of the force beyond the habits of action is the habits of thought towards cyber.

MARSOC must not allow itself to remain proficient in the present. Foresight is what puts the "lead" in leader. Therefore, MARSOC must prepare the force through condition setting requirements as outlined above for a battle that will inevitably require more delegated authorities to the lowest level. The force should not need to adjust to new authorities such as cyber offensive capabilities; it should just merely expand its scope. An operator does not omit call for fire for an AO that has restriction to indirect fire. The operator remains at the ready when the restrictions are lifted. Combat readiness is not just power that can be influenced today; rather, it is what can be influenced in the future before the tactical thinkers have thought of it. The institution must seek out the strategic thinkers, the outlier thinkers, the diversity of thought that is required to boost this groupthink prone organization. It should not require an emotional event to trigger organizational change in the way special forces think. A strategic renewal on how MARSOC views the operating environment, strategic human resource management, and strategic renewal on leadership are follow on actions that can also execute in parallel. Will MARSOC execute all that is listed above? Eventually, it will. The question is whether it enacts it through organizational change or through an imminent cyber-attack on its infrastructure and personnel. History is siding with the latter because it is emotions, not logic, that drive changes within an organization.

In conclusion, everyone sees the cyber threat around us but have no idea how to lead through the fog of war. The oldest word that can be found on leadership is *ducere.* It appeared as early as 800BC in the Bible and other Christian books. It meant "to draw, drag, pull; to lead, guide, conduct." MARSOC must draw, drag, and pull its way out of the back seat of the great power competitive fight by taking action now. Follow up success and exploit and finish by leading, guiding, and conducting their way to the tip of the front lines. Change the habits of actions toward planning, current C2 structure, and talent management and gear it to a strategic habit of thought about the future cyber kinetic warfare. The first step is for tactical leaders to generate the requirements through well scoped planning that includes cyberspace. Since structure is subtle in humans, organizational structure is needed. The second step is to structure MARSOC to best support the requirements because structure influences human behavior. The last step is to maintain a cyber force talent management as incidental cyber warriors because the knowledge gained will generate a new way of thinking that can be leveraged in combat. The target is laid before the force and it is time for direct, meaningful, substantive action that will reverberate. MARSOC cannot afford to remain static and allow another service component to take the lead if MARSOC hopes to continue its success; MARSOC must change in order to keep up with the changed world.