Cyber in the Single Battle

Antiquated operational models need to change

by Maj Dennis W. Katolin

The Marine Corps' relevance to the United States' security is success through responsiveness and adaptation. Unfortunately, the Marine Corps is posturing itself for an unlikely fight that is not yielding dividends for Americans interests. The persistent deployment of small MAGTFs is an antiquated model that centers on kinetic action in a world that increasingly blurs the line between physical and digital realms. The United States needs a force that can rapidly adapt to an operational environment that sees the proliferation of information networks changing the dynamic within countries with which the Nation is both competing and cooperating. Despite the establishment of a MEF Information Group, the Corps has no approach to integrating cyber into the MAGTF's single battle construct. The Marine Corps must develop a new doctrine on tactical information operations within the MAGTF by incorporating standardized planning approaches to cyberspace operations and strengthening the communications community, thereby creating an operations center that has a holistic approach to monitoring cyber.

Another reason for the lack of cyber integration is a misconception about the nature of cyberspace operations. A common paradigm of cyber is that it is often associated with rear area operations: large server rooms in industrialized areas that require a tremendous amount of infrastructure to power and maintain. This is logical, as cyberspace operations are the most advanced warfighting domain in terms of digital technology. This often seems to be at odds with the Marine Corps' expeditionary nature. Fundamentally, the austerity associated with most forms of amphibious operations seems to be diametrically opposed to this infrastructure-centric paradigm people have of cyberspace operations.

>Maj Katolin is the Operations Officer, 9th Communication Battalion, Camp Pendleton, CA.

This "expeditionary operations versus cyberspace operations" construct presents a false dichotomy that discourages Marine leaders from employing all assets in a warfighting domain that requires "maneuver." *Joint Publication 3-12, Cyberspace Operations*, states,

> Actions in cyberspace, through carefully controlled cascading effects, can enable freedom of action for activities in the physical domains. Likewise, activities in the physical domains can create effects in and through cyberspace by affecting the electromagnetic spectrum or the physical infrastructure.[1]

Amphibious, air, and ground operations cannot be undertaken on the modern battlefield without maneuver in cyberspace. The next step is to create a model of how to integrate all of these options into a coherent operational approach. This model must be comprehensive across doctrine, organization, training, materiel, leadership and education, personnel, and facilities.

The Marine Corps has done well in integrating actions across the sea, air, and land domains because of the three tenants of its planning process: top-down planning, integrated planning, and the single battle construct. When addressing the single battle construct, *MCWP 5-10, Marine Corps Planning Process,* states that "operations or events in one part of the battlespace often have profound and consequent effects on other areas and events."[2]

Successful employment across multiple domains, however, can only be achieved through integrated planning, which is "conducted to coordinate action toward a common purpose by all elements of the force."[3] It is here, in integrated planning, that the Marine Corps struggles with incorporating cyberspace operations into the single battle construct. There must be a better grasp of what cyberspace is and how it connects to the other maneuver elements of the MAGTF.

Bringing Cyber into the Single Battle Construct

Cyberspace operations are dynamic and require maneuver that seeks out and orients on the enemy. As author Marc Goodman states,

> Our goal can no longer be purely prevention. We must chase the ghost from our machines by proactively searching them out and hunting them down.[4]

To be successful at the tactical layer of cyber, the Marine Corps must implement critical changes and innovations to its future operations, primarily in its planning for cyberspace operations, training for its cyber operators, and incorporation of artificial intelligence to help reduce its network signatures.

First, integrate cyberspace operations into a single battle construct that incorporates cyber maneuver forces in planning the same way logistics, air, and ground forces are incorporated for operations. The Marine Corps Planning Process provides a sound framework

for this; specifically, what planners must provide is a frame of reference for the MAGTF commander's logical battlespace, points in which the physical layer of cyber impacts the rest of the MAGTF and then orient the MAGTF commander's intelligence collections and fires (kinetic and non-kinetic) within his battlespace. This starts with the joint intelligence preparation of the operating environment.

Joint Publication 2-01.3, Joint Intelligence Preparation of the Operating Environment, states,

> The operational environment (OE) is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.[5]

The first step of the joint intelligence preparation of the operating environment is to define the operating environment, specifically the areas of operation, influence, and interest. Once the operating environment is defined and described, a MAGTF commander can better understand what factors are influencing his ability to achieve his end state and where his forces have freedom of movement. Figure 1 shows a model for MAGTFs to use in the future.

Providing these boundaries (and the threats that reside within them) for a MAGTF allows a MAGTF commander to focus his limited collections assets on named areas of interest. While a MAGTF commander may only have freedom of movement within his own domains, he may be able to identify the need for joint or interagency assets in areas of influence or interest, such as servers that reside in the United States that provide logistics and maintenance support for a deployed MAGTF.

Identifying the threats within the operating environment can help a MAGTF commander understand the nature of the operation. Unlike a conventional fight where identified organizations operate in a defined geographic area, cyberspace operations are persistent, global, and well beyond nation-backed militaries or well-financed terrorist organizations. As John Fialka states in his book, *War by Other Means*, "Unlike most other forms of attack … entry into the game is extremely cheap."[6] The moment a MAGTF commander connects his domain to the DOD Information Network (DODIN), he is in a global contest against state-sponsored and trained cyber professionals in organized militaries as well as teenagers around the world who have computers, some programming skills, and too much time on their hands. MAGTFs must be able to deal with such threats along physical and logical lines.

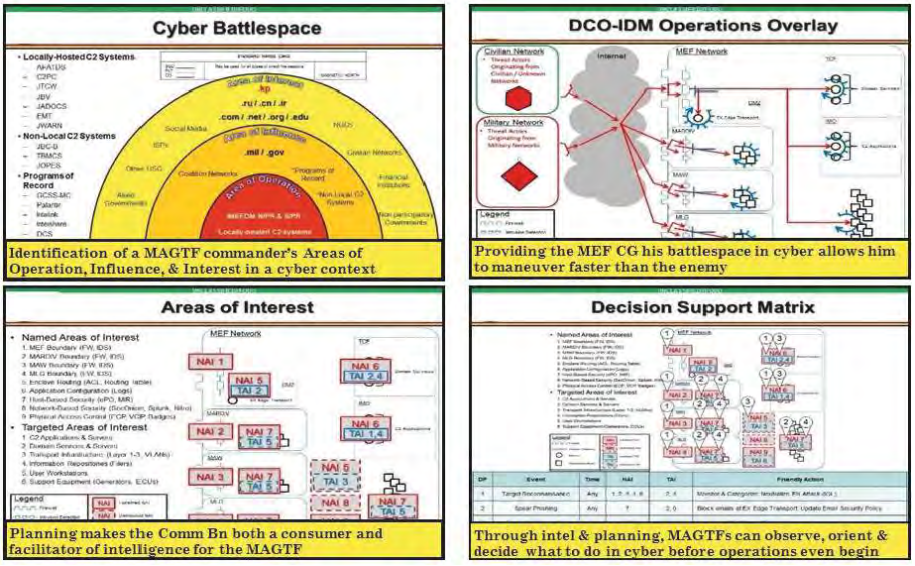

Figure 1. Cyberspace as an operating environment. **(Source: Capt John Conrad and Maj Dennis Katolin, Maneuver in All Domains, *([Oceanside, CA: May 2018].)***

In March 2018, Headquarters Marine Corps released *MARADMIN 136/18,* establishing the cyberspace 1700 occupational field. It states,

> Cyberspace operators supervise, direct, execute, synchronize, deconflict and provide guidance on the employment of cyberspace capabilities. They are the subject matter experts for the planning, development and employment of cyberspace warfare capabilities across the range of warfighting domains.[7]

While this new occupational field will help mitigate many of the Marine Corps' vulnerabilities in cyberspace, it will not be able to address cyberspace operations holistically.

A Force That Is Trained for the Fight

A holistic approach must merge logical and physical layers of cyber. This requires a fundamental shift in the Corps' communications community, the 0600 occupational field. This community has long touted that it is the cyberspace operator for the Marine Corps, but this was wrong. The 0600 community is responsible for the DODIN operations within cyberspace and operates at some of the logical layers and all of the physical layers of cyber. Unfortunately, the 0600 community focuses primarily on being network engineers who provide computer, phone, and radio support to the Corps' maneuver units. Communicators do not view themselves as maneuverists operating in the physical and logical layers of cyberspace. Consequently, they fail to understand the intelligence and targeting cycles that are vital to the MAGTF's success in cyber.

One of the biggest innovations that can occur in the communications community is doctrinally changing their mission. Communicators view success as getting the MAGTF's network online. They must realize that once the network is established, they are immediately contested by multiple enemies trying to prevent the MAGTF from succeeding. Tactical unit communicators must move beyond focusing exclusively on facilitating the command and control of others and start viewing themselves as critical MAGTF operators within information warfare and cyberspace.

Observing Cyber and Connecting It to Physical Maneuver

Once the role of Marine communicators accurately reflects that they are operators in the cyber domain, their training pipeline must require them to speak the language of planning, intelligence, and targeting as proficiently as anyone else in the MAGTF. Just as infantry officers know about the capabilities of BTR-80s that maneuver against them, or a pilot's ability to understand how a SA-20 can shoot them out of the sky, communicators need to understand the enemy's ability to use a botnet to attack the logical layer of the MAGTF's network or to employ an SU-24 to target satellite terminals.

The unit best suited to plan for intelligence and targeting against these physical and logical layers is the communication battalion. *MCIP 3-40.02, Marine Corps Cyberspace Operations,* states that the communication battalion is "the senior MAGTF organization that conducts cyberspace operations."[8] The battalion is formally responsible for two of the three lines of operation within cyberspace operations: DODIN operations and defensive cyberspace operations.[9] Having DODIN and defensive cyber operations under one commander achieves unity of command for the MAGTF in cyber.

Once under the same command, DODIN operations and defensive cyberspace operations require a cell to harmonize their efforts. To do this, the Marine Corps must adopt the Expeditionary Network Defense Operations Center (ENDOC). The ENDOC must be an operations center that integrates all staff functions to assess potential threats to the network through research on enemy threat capabilities and analysis of actions on the network (see Figure 2). Its role must be to inform the communication battalion and MIG commanders of any actions on the network that are consistent within enemy threat capabilities or any other potential compromise to the network and recommend appropriate responsive action (from any component of the MAGTF) to mitigate that threat. The ENDOC should also facilitate planning for future MAGTF operations that could require support from the communication battalion.

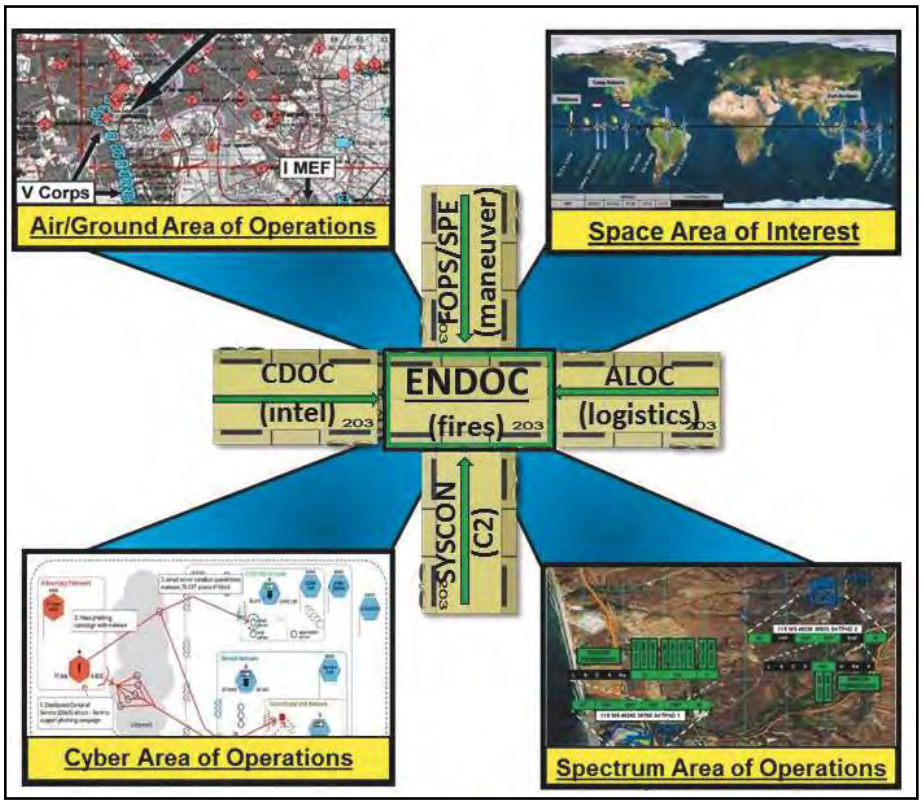

Figure 2. The ENDOC's fusion for the MAGTF. *(Source: Capt John Conrad and Maj Dennis Katolin,* **Maneuver in All Domains,** *[Oceanside, CA: May 2018].)*

Performing these tasks will provide MAGTF commanders with resilient networks. Goodman defines network resilience as

> one that will not fail catastrophically but degrade slowly over time until it can be repaired. A resilient system will continue to perform its most critical functions, though other less important activities may go off-line or cease to operate.[10]

To fulfill these tasks, the ENDOC needs to perform three functions.

Functions of the ENDOC

The first function must be the persistent assessment of the physical threats to the network. With enemy threats of jamming, sabotaging power infrastructure, and reconnaissance, the communication battalion must maintain awareness of actions within the area of operations that may indicate a threat to its physical infrastructure. Additionally, the MAGTF's reliance on space and spectrum requires subject matter experts who help engineer the network to speak to these issues. The ENDOC will bring in members of the system planning engineering cell, systems control, and battalion staff to assess what physical compromises will keep them from facilitating command and control for the MAGTF commander.

Another overlooked aspect to the physical layer of cyberspace is power. For an expeditionary fighting force operating in an austere environment, fuel for generators that power the network is at a premium. Tactical expeditionary cyberspace operators must measure bandwidth, not just in data rates but in gallons. As Goodman states, "Much of our technological infrastructure is subject to common single points of failure, the most obvious of which is power. No electricity, no Internet."[11]

The ENDOC must have a logistics wing that assesses engineering, sustainment, and maintenance of the network's power infrastructure.

The ENDOC's second function must be to analyze logical threats to the

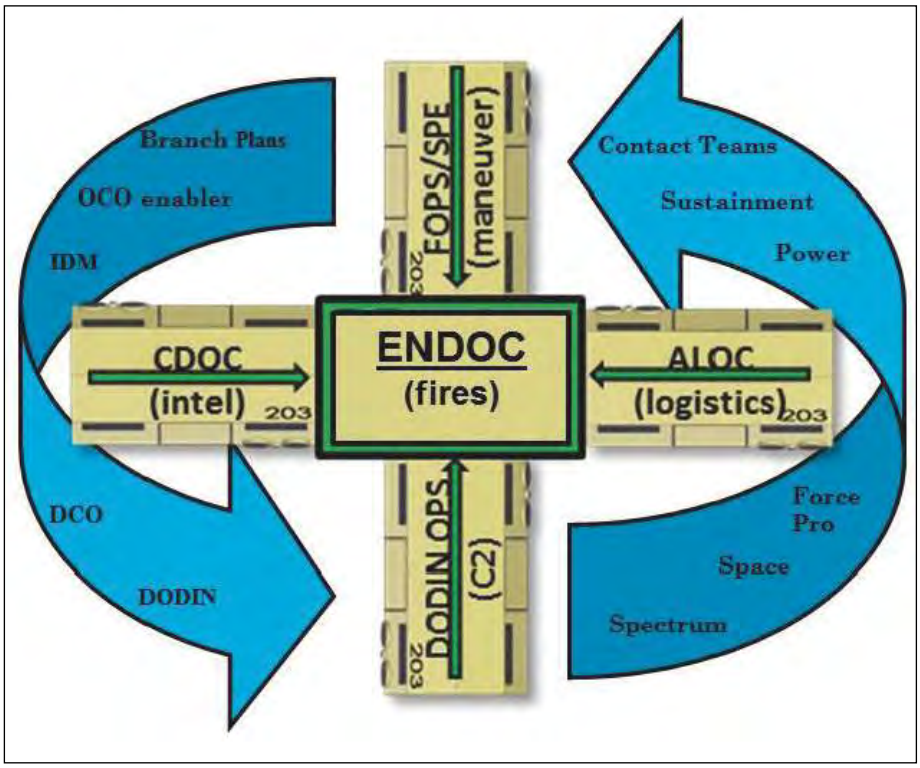

Figure 3. The ENDOC's cyclical approach to cyberspace. *(Source: Capt John Conrad and Maj Dennis Katolin,* **Maneuver in All Domains,** *[Oceanside, CA: May 2018].)*

MAGTF's network. With cyberspace maturing as a warfighting domain, the battalion must be prepared to rapidly assess and analyze actions (both friendly and enemy) within cyberspace. The ENDOC is a medium to generate and provide cyber network analysis to the MEF Information Group. This function is performed in a variety of ways. One provides recommendations for named areas of interest for cyberspace intelligence collections. Another analyzes raw data from the systems control center and help desks to determine if network issues are indications of enemy actions on our network or routine outages that normally occur with expeditionary networks.

The ENDOC's third function must be to help facilitate cyber considerations for future planning within the MAGTF. The ENDOC will help monitor current plans for the MEF/MEF (Forward) and assess any future operations (occurring within a 96-hour window) within the MAGTF that may require support from the communication battalion. The ENDOC will gather representatives from the commanders and staff to assess what administrative, personnel, logistical, or communications support the battalion can provide (and what supplementary assistance it would need to provide that support). Figure 3 shows the cyclical nature of information synchronization within the ENDOC.

The ENDOC allows the communication battalion to be the MAGTF sensor within the cyber domain that best facilitates the ability of intelligence and radio battalions to quickly assess the actions on the network and determine if they are physical, logical, friendly, or enemy. Only the communication battalion has the expertise to perform all three functions of the ENDOC. The ENDOC is the only organization within the MEF that is qualified and poised to leverage that expertise to harness raw data from across the network, analyze it into processed data, translate it into actionable knowledge about actions within cyberspace, and recommend what should be done to resolve it, as depicted in Figure 4.

Conclusion

The Marine Corps must modernize its single battle concept. Its focused role within the DOD and legacy of innovation will propel the Corps toward maneuver in this new warfighting domain. Once the institution's paradigm shifts toward cyber in its single battle, the Marine Corps will have a force that is

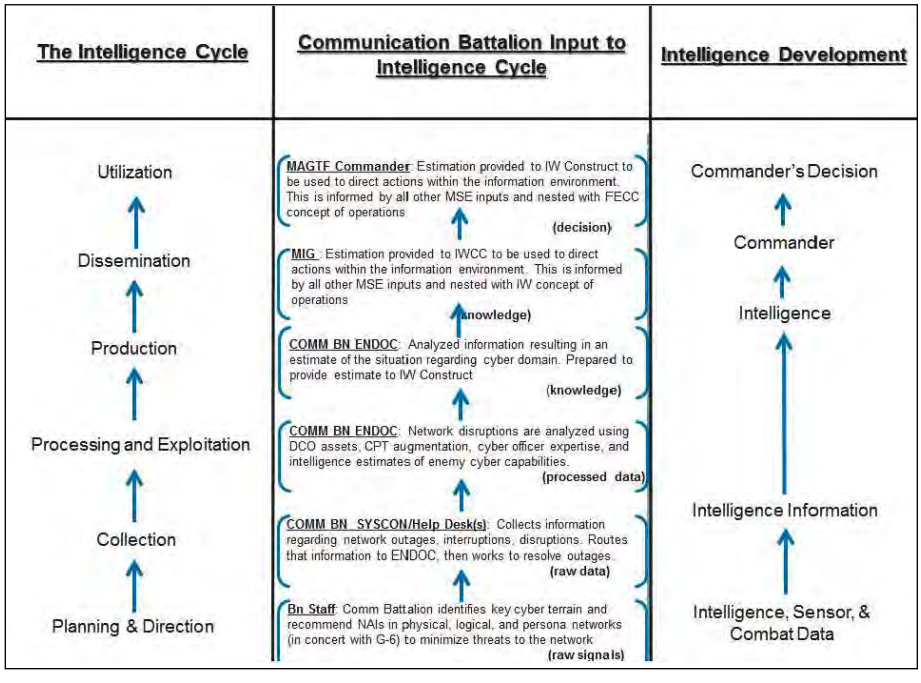

Figure 4: The ENDOC's parallel to the intelligence cycle. *(Source: Dennis Katolin,* **Seize the Initiative,** *[October 2017].)*

able to maneuver in support of political policy. The Corps must steer away from the false dichotomy that technology is counter productive to operating in austerity and release a new doctrine of "tactical cyber." Just as it did with the *Tentative Manual for Landing Operations* in 1936 and the *Small Wars Manual* in 1940, the Marine Corps will write a new chapter for America's military regarding the employment of cyberspace and information operations at the tactical level. This philosophical approach will fulfill a gap for the DOD and show that a sustainable, expeditionary fighting force can rapidly apply these new concepts in a single battle construct and facilitate success for the joint force.

Notes

1. Joint Chiefs of Staff, *Joint Publication 3-12, Cyberspace Operations*, (Washington, DC: February 2013).

2. Headquarters Marine Corps, *MCWP 5-10, Marine Corps Planning Process*, (Washington, DC: May 2016).

3. Ibid.

4. Marc Goodman, *Future Crimes: Inside the Digital Underground and the Battle for Our Connected World*, (New York, NY: Penguin Random House Publishing, 2015).

5. Joint Chiefs of Staff, *Joint Publication 2-01.3, Joint Intelligence Preparation of the Operating Environment*, (Washington, DC: April 2018).

6. John Fialka, *War by Other Means: Economic Espionage in America*, (New York, NY: W.W. Norton Publishing, 1999).

7. Commandant of the Marine Corps, *MARADMIN 136/18, Establishment of the Cyberspace Occupational Field*, (Washington, DC: March 2018).

8. Headquarters Marine Corps, *MCIP 3-40.02, Marine Corps Cyberspace Operations*, (Washington, DC: October 2014).

9. Ibid.

10. *Future Crimes.*

11. Ibid.