The Cyber Base of Fire

A combined arms approach to cyber maneuver

by Maj Paul L. Stokes & LtCol Barian A. Woodward

> *"The base of fire covers the maneuver element's advance toward the enemy position by engaging all known or suspected targets. Upon opening fire, the base of fire seeks to gain fire superiority over the enemy. Fire superiority is gained by subjecting the enemy to fire of such accuracy and volume that the enemy fire ceases or becomes ineffective."*
>
> **—MCRP 3-10A.3, Marine Rifle Squad, *2 May 2016*[1]**

The Marine Corps' contribution to the national defense has successfully evolved throughout its history by virtue of the ability of Marines to identify and adapt to the Nation's national security needs, often before those needs were commonly recognized. Such innovations as the seizure and defense of advanced naval bases, amphibious operations, close air support, helicopter-borne vertical envelopment tactics, maritime pre-positioning forces, and task-organized, combined arms forces consisting of aviation, ground, and logistic elements known as MAGTFs are prime examples of how the Marine Corps has adapted and evolved as an expeditionary force. The Marine Corps continually reviews its roles and missions in the context of an uncertain world, adapting to the changing security needs of the Nation while preserving those core values and professional capabilities that make Marines succeed in war and peace.[2]

This institutional mindset of innovation, when applied to the fifth and six warfighting domains of cyberspace[3] and the ESM (electromagnetic spectrum),[4] provides us, as Marines, with a rare opportunity to develop a combined arms approach to cyberspace and EMSO (EMS operations) that can support all levels of the MAGTF and joint and combined operations as well as provide a foundation for the information warfare (IW) doctrine[5] currently being developed by the DC, CD&I (Deputy Commandant, Combat Development & Integration).

While that may seem to be a daunting task, all one has to do is look at the Marine Corps baseline maneuver element—the Marine rifle squad—to recognize the fact that we have the knowledge and manpower right at our fingertips to transform this concept into a reality.

The Challenge

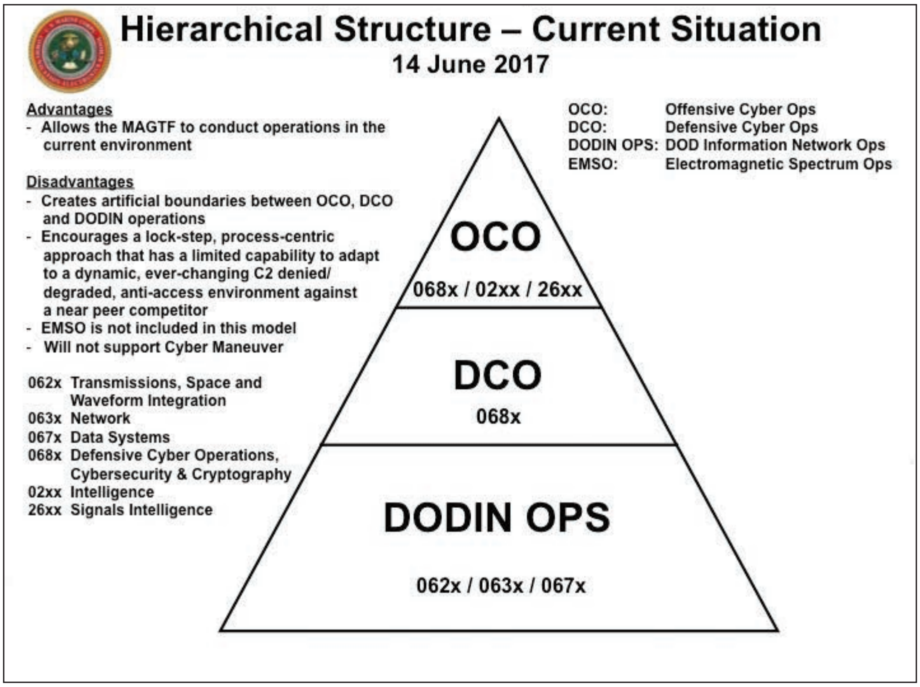
The six Marine Corps warfighting functions,[6] C^2 (command and control), maneuver, fires, intelligence, logistics, and force protection, are all heavily dependent upon cyberspace and EMSO, which requires both cultural and organizational changes in how we approach cyber maneuver. Cultural in the sense that every Marine in the MAGTF must embrace the fact that effective C^2 is dependent on his actions, and organizational in the sense that a MAGTF commander must be prepared to task organize his cyber/EMSO elements—in the same manner that a Marine squad employs his three maneuver elements (i.e., his three fire teams)—into a "cyber base of fire" (CBF) that is fully capable of maintaining, protecting, and dominating the cyberspace/EMSO battlespace.

Where We Are Today

Current Marine Corps cyber/EMSO doctrine is based on a top-down, hierarchical structure. (See Figure 1 on next page.) At the top are offensive cyber operations (OCO), which are cyber-

>Maj Stokes: See page 18 for bio.

>>LtCol Woodward, a former Marine Staff Sergeant Small Computer Systems Specialist with over 26 years of service, is currently serving as the CO, Communications Training Battalion, Marine Corps Communication-Electronics School, and is responsible for all 06xx MOS officer and enlisted training.



Hierarchical Structure – Current Situation
14 June 2017

Advantages
- Allows the MAGTF to conduct operations in the current environment

Disadvantages
- Creates artificial boundaries between OCO, DCO and DODIN operations
- Encourages a lock-step, process-centric approach that has a limited capability to adapt to a dynamic, ever-changing C2 denied/degraded, anti-access environment against a near peer competitor
- EMSO is not included in this model
- Will not support Cyber Maneuver

062x	Transmissions, Space and Waveform Integration
063x	Network
067x	Data Systems
068x	Defensive Cyber Operations, Cybersecurity & Cryptography
02xx	Intelligence
26xx	Signals Intelligence

OCO:	Offensive Cyber Ops
DCO:	Defensive Cyber Ops
DODIN OPS:	DOD Information Network Ops
EMSO:	Electromagnetic Spectrum Ops

Figure 1.

space operations missions intended to project power in and through foreign cyberspace via actions taken in support of the combatant commander or national objectives.[7] In the middle are defensive cyber operations (DCO), which are passive and active defense missions intended to "preserve the ability to utilize friendly cyberspace capabilities and protect data," cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent malicious cyberspace activity.[8]

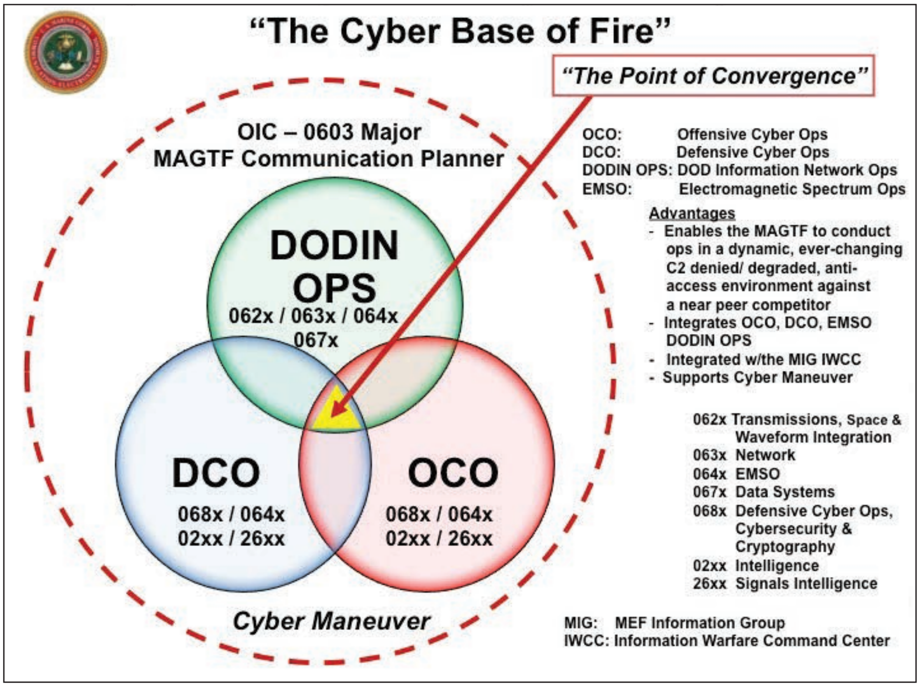
At the bottom are DODIN (DOD information network) operations, which are actions to secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the security of the DOD information network.[9]

While the hierarchical structure does allow the MAGTF to conduct operations in a variety of venues, it is fundamentally flawed because it creates artificial boundaries between OCO, DCO, and DODIN operations—encouraging a lock-step, process-centric approach to cyberspace maneuver that has limited capacity to adapt to a dynamic, ever-changing, C^2 denied/degraded, anti-access environment when we're fighting a near-peer competitor. Furthermore, EMSO is not integrated in this model, which means that any coordination between "the three tiers" and the MAGTF EMS personnel must be completed on an ad hoc basis, which is a prescription for disaster in a future war.

Where We Need To Be

Maneuver is defined as

> the movement of forces for the purpose of gaining an advantage over the enemy in order to accomplish an objective. That advantage may be psychological, technological or temporal as well as spatial. Maneuver is movement relative to the enemy to put him at a disadvantage. It normally includes the movement of forces on the battlefield in combination with fires. Maneuver is the dynamic element of combat and the means of concentrating forces for decisive action to achieve the surprise, psychological shock, physical momentum, and moral dominance that enables smaller forces to defeat larger ones. Commanders



"The Cyber Base of Fire"

"The Point of Convergence"

OIC – 0603 Major
MAGTF Communication Planner

DODIN OPS
062x / 063x / 064x
067x

DCO
068x / 064x
02xx / 26xx

OCO
068x / 064x
02xx / 26xx

Cyber Maneuver

OCO: Offensive Cyber Ops
DCO: Defensive Cyber Ops
DODIN OPS: DOD Information Network Ops
EMSO: Electromagnetic Spectrum Ops

Advantages
- Enables the MAGTF to conduct ops in a dynamic, ever-changing C2 denied/ degraded, anti-access environment against a near peer competitor
- Integrates OCO, DCO, EMSO DODIN OPS
- Integrated w/the MIG IWCC
- Supports Cyber Maneuver

062x Transmissions, Space & Waveform Integration
063x Network
064x EMSO
067x Data Systems
068x Defensive Cyber Ops, Cybersecurity & Cryptography
02xx Intelligence
26xx Signals Intelligence

MIG: MEF Information Group
IWCC: Information Warfare Command Center

Figure 2.

> maneuver their forces to create the conditions for tactical and operational success. Forces may maneuver in other dimensions as well. For instance, a force may also maneuver in time by increasing relative speed and operating at a faster tempo than the enemy.[10]

By task organizing his organic cyber, EMSO, intelligence, and signals intelligence personnel, a MAGTF commander can create a CBF that will enhance his ability to successfully maneuver in cyberspace and the EMS and fix/strike/defeat the enemy with cyber and electronic fires as well as defend his C^2 networks.

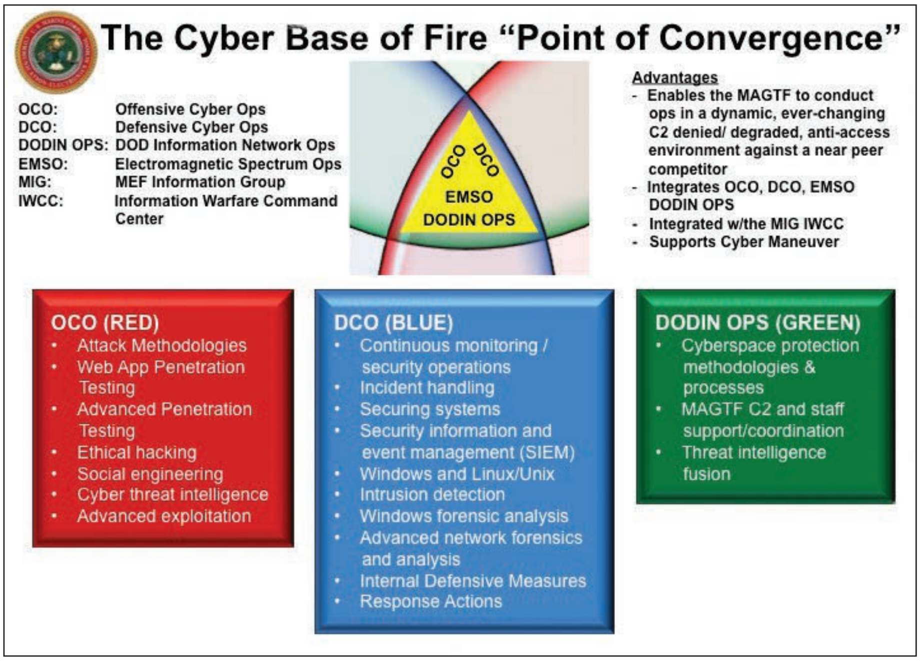
Using existing fire support doctrine as a guide, the CBF would be comprised of three mutual supporting sections—DODIN operations, DCO, and OCO—and collocated with the MAGTF command element. (See Figure 2.)

The CBF would serve as the "point of convergence" wherein the activities of DODIN operations, DCO, OCO, EMSO, and electronic/spectrum warfare are coordinated and synchronized in accordance with MAGTF mission requirements. Furthermore, it would improve the relationships between the MAGTF commander and external agencies like U.S. Marine Corps Forces Cyberspace, the Defense Information Systems Agency, and the supported combatant command by creating an electronic fire coordinator[11] responsible for all cyber/EMSO activities in support of the MAGTF. (See Figure 3.)

CBF Composition

The DC, CD&I-approved modernization of the 06xx (Communications) occupational field[12] provides us with a golden opportunity to implement the CBF concept because it has spread the routine cybersecurity responsibilities out across the 06xx workforce. As of October 2017, the new 06xx MOS[13] responsibilities now include:

- 062x and 064x, Transmissions, Space, and Waveform Integration, EMSO
  - IP networking
  - Electromagnetic spectrum challenges/mitigation
  - Spectrum management
  - Space operations considerations
- 063x Network
  - Layer 4 and below cybersecurity measures
    - Firewalls
    - Intrusion Detection Systems (IDS)/Intrusion Protection Systems (IPS)
- 067x Data Systems
  - Layer 5 and above cybersecurity measures
    - Public key infrastructure
    - Host-based security systems
    - Assured compliance assessment solution
- 068x Defensive Cyber Operations, Cybersecurity, and Cryptography
  - DCO Internal Defensive Measures (DCO-IDM)



The Cyber Base of Fire "Point of Convergence"

OCO: Offensive Cyber Ops
DCO: Defensive Cyber Ops
DODIN OPS: DOD Information Network Ops
EMSO: Electromagnetic Spectrum Ops
MIG: MEF Information Group
IWCC: Information Warfare Command Center

OCO DCO
EMSO
DODIN OPS

Advantages
- Enables the MAGTF to conduct ops in a dynamic, ever-changing C2 denied/ degraded, anti-access environment against a near peer competitor
- Integrates OCO, DCO, EMSO DODIN OPS
- Integrated w/the MIG IWCC
- Supports Cyber Maneuver

OCO (RED)
- Attack Methodologies
- Web App Penetration Testing
- Advanced Penetration Testing
- Ethical hacking
- Social engineering
- Cyber threat intelligence
- Advanced exploitation

DCO (BLUE)
- Continuous monitoring / security operations
- Incident handling
- Securing systems
- Security information and event management (SIEM)
- Windows and Linux/Unix
- Intrusion detection
- Windows forensic analysis
- Advanced network forensics and analysis
- Internal Defensive Measures Response Actions

DODIN OPS (GREEN)
- Cyberspace protection methodologies & processes
- MAGTF C2 and staff support/coordination
- Threat intelligence fusion

Figure 3.

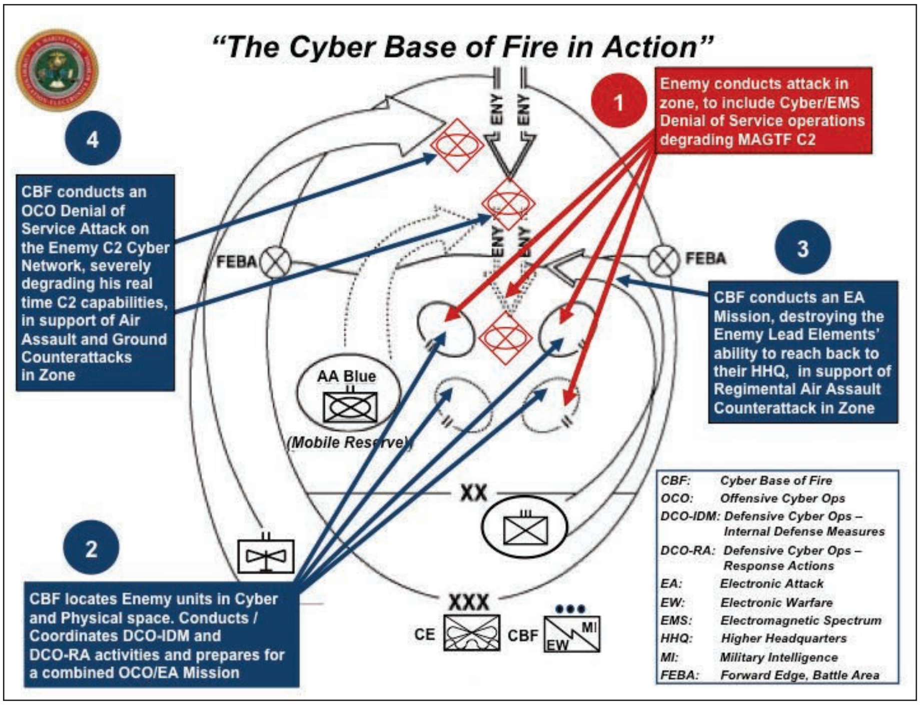

"The Cyber Base of Fire in Action"
1
Enemy conducts attack in zone, to include Cyber/EMS Denial of Service operations degrading MAGTF C2
2
CBF locates Enemy units in Cyber and Physical space. Conducts / Coordinates DCO-IDM and DCO-RA activities and prepares for a combined OCO/EA Mission
3
CBF conducts an EA Mission, destroying the Enemy Lead Elements' ability to reach back to their HHQ, in support of Regimental Air Assault Counterattack in Zone
4
CBF conducts an OCO Denial of Service Attack on the Enemy C2 Cyber Network, severely degrading his real time C2 capabilities, in support of Air Assault and Ground Counterattacks in Zone
ENY
ENY
ENY
ENY
FEBA
FEBA
AA Blue
(Mobile Reserve)
XX
XXX
CE
CBF
MI
EW
CBF: Cyber Base of Fire
OCO: Offensive Cyber Ops
DCO-IDM: Defensive Cyber Ops – Internal Defense Measures
DCO-RA: Defensive Cyber Ops – Response Actions
EA: Electronic Attack
EW: Electronic Warfare
EMS: Electromagnetic Spectrum
HHQ: Higher Headquarters
MI: Military Intelligence
FEBA: Forward Edge, Battle Area

Figure 4.

- DCO-Response Actions (DCO-RA)

• 0699 Supervise and Coordinate Communications and 0602/3/5 Management of Communications and Cybersecurity

- Cyberspace operations
- EMSO
- Space operations

By distributing these skills throughout the 06xx community, the MAGTF commander now has the 06xx Marines he needs to establish the three elements of the CBF. And when paired up with 02xx Intelligence and 26xx Signals Intelligence Marines in each element of the CBF, he will possess the synergy he requires to effectively seek out, close with, and destroy the enemy within the cyber/EMSO domains, as well as protect his ability to exercise C^2.

The CBF in Action

In Figure 4, a reinforced enemy mechanized task force is depicted conducting a coordinated attack, to include cyber/EMS denial of service operations, which has resulted with a deep penetration into the MAGTF's zone of action.

In response, the CBF "combined arms team" of communicators (06xx), intelligence analysts (02xx), signals intelligence experts (26xx), and possibly cyber (17xx)[14] experts begin to locate and assess enemy units in both cyber and physical space. Concurrently, they institute DCO-IDM and DCO-RA activities that enable the MAGTF to restore critical C^2 links while coordinating with the appropriate authority (i.e., Combatant Command, Marine Forces Cyber, and/or the Defense Information Systems Agency) in preparation for a combined OCO/electronic attack[15] mission in support of a regimental-sized air assault counterattack.

On order, the CBF officer-in-charge, a major 0603, MAGTF Communications Planner, maneuvers his OCO section and executes an electronic attack mission and OCO denial of service attack on the enemy C^2 cyber network—*severely degrading his real-time C^2 capabilities*—in support of the MAGTF's combined air assault and ground counterattacks in zone while ensuring that these electronic fires have no impact on friendly forces.

In a matter of seconds, the enemy commander is faced with a complete loss of voice and data connectivity to both his higher headquarters and maneuver elements, which has the effect of completely derailing his timetable. Within seconds, it is obvious that the situation has done a complete 180°, and it is now his turn to "pay the butcher's bill" as he watches his lead battalions disappear in the fire and smoke of coordinated air strikes/barrages from Marine F-35B Lightning IIs, AV-8B Harriers, and artillery.

The Future

A question that comes to mind is: Do we have the Marines and the training establishment we need to train, equip, and field the CBF? The short answer is "yes" in the long term, but in the short term, there are a number of planning factors and decision points that have to be considered and/or rectified.

• The cyberspace/EMSO training continuum needs to be streamlined and managed by the MCCES (Marine Corps Communication-Electronics School). After all, MCCES' mission is

> to train Marines in ground electronics maintenance, communications, and aviation command and control operations and maintenance in order to ensure commanders at all levels have the ability to exercise command and control across the full range of military operations.[16]

Do we have the Marines and the training establishment we need to train, equip, and field the CBF?

This includes cyberspace operations, a subset of communications; therefore it only makes good sense—from a Service-wide perspective—to provide MCCES the resources it needs to train 06xx, 02xx, 26xx, and 17xx Marines in DODIN operations, DCO, and OCO.

• The CBF supports the MIG (MEF Information Group) information warfare IWCC (information warfare command center)[17] by outlining the roles and responsibilities of DODIN operations, DCO, and OCO and how they come together in support of cyber maneuver. The IWCC is being tested in wargames and exercises, and with time, many of the friction points between the radio, intelligence, and communication battalions will be worked out—thereby ensuring that all elements of the MIG are involved in supporting the MAGTF commander's intent and mission.

- The command relationships/authorities that govern DODIN operations, DCO, and OCO need to be streamlined in order to support a MAGTF commander operating in a dynamic C^2 denied/degraded, anti-access environment. It is simply impractical and unrealistic to expect a forward deployed MAGTF commander to reach all the way back to the National Capitol Region to obtain permission to conduct an OCO mission—especially when that connectivity may not exist because of enemy action. The CBF provides the MAGTF commander with the trust/expertise he requires to conduct cyber maneuver in his battlespace; all that is required is the appropriate authority/permissions to do so.

... the CBF OIC employs/maneuvers his cyber combined arms team in support of the MAGTF commander.

- In addition to the above, the 06xx community needs to reexamine this issue during the next MOS manual review cycle.
  - ■ The creation of an 0680 DCO warrant officer career track. The current 06xx FMP (Force Modernization Plan) does not include a 0680 DCO warrant officer. This inhibits the MAGTF's ability to counter and defeat enemy cyber threats in the future.
  - ■ The consolidation of the 0620 space and waveform integration officer and 0640 strategic electromagnetic spectrum officer warrant officer MOS tracks into a single MOS. As we expand the integration of cyber/EMSO into MAGTF operations and consolidate all 06xx training at MCCES, it is impractical to retain two warrant officer MOSs that, in many respects, are performing the same duties. Therefore, it is time to consolidate these two MOSs into one while retaining the overall structure.

It's Time to Seize the Initiative

In the same manner that a Marine rifle squad leader employs his Marines as a base of fire in order to gain fire superiority over the enemy, the CBF OIC employs/maneuvers his cyber combined arms team in support of the MAGTF commander. The CBF concept is based on the proven principles of war and will prepare the Marine Corps for the cyber/EMSO challenges of the future. All that is required is the willingness and tenacity to seize the initiative and make it happen.

Notes

[1] Headquarters Marine Corps, *MCRP 3-10A.3*, (formerly *MCWP 3-11.2*), *Marine Rifle Squad*, (Washington, DC: 2 May 2016).

[2] Headquarters Marine Corps, *MCDP 1-0*, *Marine Corps Operations*, (Washington, DC: 27 September 2001).

[3] Deputy, Secretary of Defense Memorandum, Subject: Definition of Cyberspace, 12 May 2008: Cyberspace is defined as a "global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the internet, telecommunications networks, computer systems, and imbedded processors and controllers."

[4] Department of Defense, *DOD Directive 3610,aa Electromagnetic Spectrum Operations (EMSO) Policy (draft)*, Office of the Chief Information Officer, (Washington, DC: draft), recognizes "the EMS as an operational domain comprised of all electromagnetic energy."

[5] MEF Information Group, *Marine Air-Ground Task Force (MAGTF) Information Warfare Concept of Employment,* (Quantico, VA: Deputy Commandant, Combat Development & Integration (DC, CD&I), draft 10 May 2017).

[6] *MCDP 1-0.*

[7] Joint Staff, *Joint Publication 3-12, Cyberspace Operations*, (Washington, DC: revision final coordination draft, May 2017).

[8] Ibid.

[9] Ibid.

[10] *MCDP 1-0.*

[11] Maj Paul L. Stokes, "The Electronic Fire Support Coordinator," *Marine Corps Gazette*, (Quantico, VA: April 2011). This article explains how a Marine Communications Officer can improve his ability to support combat operations by becoming "an operator/tactician" vice remaining in his comfort zone as "the technical guy."

[12] LtGen Robert S. Walsh, approval endorsement of Director, C4, Memo Ser 5000 C4, dated 17 February 2016; Subject: Execution of HQMC C4 06xx Force Modernization Plan (FMP).

[13] Headquarters Marine Corps, *NAVMC 3500.56C, Communications Training and Readiness Manual (06xx Military Occupational Specialty)*, (Washington, DC: 2 November 2016).

[14] As of the writing of this article, 30 May 2017, the Commandant of the Marine Corps directed that the HQMC staff look into the possibility of creating a cyber occupational field (17xx) in support of OCO.

[15] Joint Staff, *Joint Publication 3-13.1, Electronic Warfare*, (Washington, DC: 25 January 2007); the term "electronic attack "has replaced the term "electronic countermeasures."

[16] LtGen Robert S. Walsh, approved mission statement for Marine Corps Communication-Electronics School, Training Command, (Twentynine Palms, CA: 30 November 2016).

[17] *MAGTF Information Warfare Concept of Employment.*