Defensive Cyberspace Operations

The integration of the defensive cyberspace operations-internal defensive measures companies

by MGySgt William W. Hess & GySgt Robert M. Moore

>MGySgt Hess is the Defensive Cyber Operations Chief, 1st Marine Expeditionary Force G6, Camp Pendleton.

>>GySgt Moore is an instructor with the Defensive Cyber Operations Training Section, Co D, Communications Training Bn, Marine Corps Communication-Electronics School, Twentynine Palms.

With the establishment of Marine Forces Cyber Command (MARFORCYBER) and the creation of the Cyber Mission Forces (CMF), the Marine Corps continues to develop and mature its cyber capabilities. Through this maturity, the Marine Corps has begun the process of pushing cyber capabilities to elements outside of the team capabilities provided by the CMF. Cyberspace operations include DODIN Ops (DOD Information Network Operations), OCO (Offensive Cyberspace Operations), and DCO (Defensive Cyberspace Operations).[1] DODIN Ops serve as the "install, operate, maintain, and secure" operations that allow Marine Corps units to develop and utilize cyber capabilities to support air, sea, and land operations.[2] OCO is an offensive capability that resides solely within the CMF teams in support of MARFORCYBER and United States Cyber Command[3] and, while mature in nature, is not quite ready for prime time within the Operating Forces (mostly due to Presidential authorities). The expanded capability that has been developed, cultivated, and is ultimately ready to be established within the Marine Corps at large is DCO. DCO includes Internal Defensive Measures (IDM) and response actions.[4 5 6] IDM utilizes the capabilities provided through DODIN Ops and the integration of cyber threat intelligence to increase the protection of key terrain in cyber to ensure mission success.[7 8 9] Using IDM, technicians are able to manipulate current security controls to identify adversarial actions within DOD networks and defend against them through security control manipulation and/or policy adjustment. Response actions allow these same technicians to respond to adversarial actions external to the boundary and ultimately stop an active attack once identified through hunt operations.[10 11] IDM and response actions allow DCO to be an effective active defense component the Marine Corps can utilize within its Operating Forces to ensure the protection of systems and information within a contested environment.[12]

The first push of cyberspace capabilities to the Operating Forces is coming in the form of DCO-IDM (Defensive Cyberspace Operations-Internal Defensive Measures) companies established at each of the three MEFs.[13] These three companies will include the necessary personnel to provide the IDM capability to the MEF commanders and ensure that the Marine Corps Operating Forces are equipped to fight future battles as the use of technology advances. The DCO-IDM company, an asset organic to communications battalions under Future Force 2025, is a critical component to integrated information operations. In order to integrate Information Warfare (IW), the MEF Headquarters Group has transitioned into a MEF Information Group (MIG). The MIG coordinates and employs information operations in support of the MAGTF. The assets of the MIG include communications and radio battalions, intelligence battalions, and a MEF support battalion. The MIG commander serves as the senior information operations officer and is also responsible for manning, training, and equipping the MEF to execute information operations. This article will provide a glimpse into the initial operational capabilities of these three companies as well as a vision for the concept of employment that will govern and task this new unit. The final operational capability for these teams will create a picture of their overall use and of the Marine Corps' cyberspace operational capacity.

Initial Operational Capability

The parameters for the initial op-

erational capability of the DCO-IDM companies are loose in their inception in order to allow the individual MEFs the freedom of maneuver to establish this capability to meet the needs of their specific mission sets. The recommended initial staffing goals as well as the training requirements and timelines will paint the picture of what these companies should look like within each MEF. Initial discussions on the purpose of these companies and their evaluation metrics will shape the future concept of employment as this capability matures. This section provides the actual missions and tasks accomplished by the personnel staffed within these companies and delves into the concept of employment.

Following the guidance of HQMC and MARFORCYBER, each MEF was tasked with identifying five to seven Marines to serve as the initial staff for the establishment of the DCO-IDM companies by December 2017.[14] The MOS selected to support this initial training was the 0688 (Cybersecurity Technician) or 0689 (Cybersecurity Chief). Since the rank requirement was not established, each of the MEFs had the latitude to decide their own team construct based on the personnel available. The MOS restrictions served to allow the staffing of these companies to be primarily 0688/89s, who will become the DCO technicians and chiefs within the Marine Corps beginning in fiscal year 2019.

Aside from the restrictions imposed, there was limited guidance with regard to qualifications. Simply possessing the proper MOS and at least a secret clearance was the only guidance prescribed by higher headquarters.[15] This prompted questions regarding the selection of these Marines and their training. Each of these Marines should have received a two-week training package from MARFORCYBER with a two-day certification process upon completion of the training.[16] The training for these Marines includes initial training, on-hand training, over-the-shoulder training with a Cyber Protection Team while on mission in the respective MEF's area of operations, and a training course that will help to solidify what their capabilities will be. The identification and training of these Marines creates the initial capability within each of the MEFs.

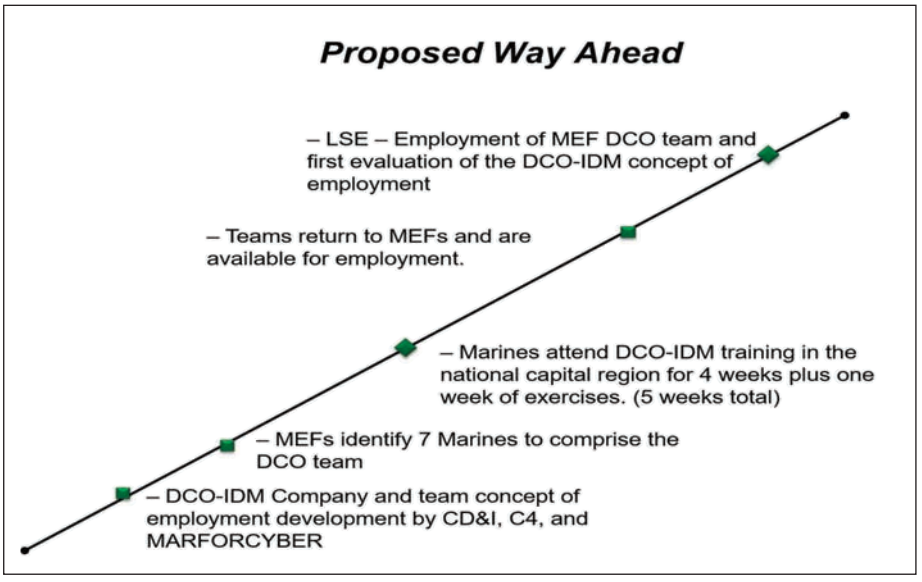


Figure 1. Timeline for Initial Operational Capability for creation of the Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM) companies.[18]

After these five to seven Marines were identified within each MEF, they were assigned to communications battalions (7th, 8th, and 9th) for further development. The communications battalions are responsible for the day-to-day tasking and utilization of these assets to ensure proper implementation across the MAGTF. Once these Marines' initial training was completed, their on-hand training took place during the I MEF exercise in March.[17] The DCO-IDM wargame conducted by HQMC was also scheduled for March, combining members from each of the MEFs to develop and test capabilities and define a concept of operations for the continued expansion and development of these units. Figure 1 shows the progression timeline for the IOC implementation of the DCO-IDM companies.

The limitation of workforce (only seven Marines) and the limited training of these Marines is a point of discussion regarding the validity of their proof of concept and probability of success based on the needs of the MEF. The after-action and lessons learned input from the initial operational capability will be critical in the development of this asset for the Marine Corps. The appetite for these companies and the capability within the MEFs is extremely high, but the old adage "the devil is in the details" holds true. The concept of employment will be vital for the future success of these units. Continued growth depends on the outcome of this initial operational capability and the concept of employment utilized to provide proper direction.

Concept of Employment

In order for any unit within the Marine Corps to be effective, its mission scope and resources must be clearly defined. In the case of the DCO-IDM companies, the Marine Corps has created a requirement based on cyber protection teams, which support the cyber mission force (CMF) within MARFORCYBER.[19] These cyber protection teams serve as the blueprint for the capabilities requested by each of the MEFs and as a necessity to match the abilities of current peer and near-peer cyber adversaries.[20] [21] [22] The employment of these companies will provide the means within each MEF to perform true active cyber defense and provide the freedom of maneuver necessary to accomplish the mission.[23] [24] [25] The following paragraphs outline a proposed concept of employment by which the Marine Corps can begin to employ this new capability in a way

that not only accomplishes the mission but also advances the expansion of cyberspace operations into the Operating Forces.

The construct of the DCO-IDM companies includes approximately 100 total Marines depending on the MEF and the missions assigned.[26] The Marines will vary in MOS and rank with the preponderance being the 0688/89 (DCO Technician/Chief). The skill sets (MOS) that these Marines possess will encompass the requirements set forth by MARFORCYBER and U.S. Cyber Command, to include the knowledge, skills, and abilities of the cyber protection teams which support the CMF. The DCO skills taught to each 0688/89 allow for a completely focused Marine, capable of performing all tasks associated with the DCO-IDM companies and the cyber protection teams.[27] Additional MOSs depend entirely on where the companies will ultimately reside. These additional MOSs may include intelligence analysts and operators, data systems and networking Marines/chiefs, and officer leadership in the form of 0602 Communications Officers, 0603 MAGTF Communications Planning Officers, or 0605 Cyberspace Operations Officers (limited duty officers) to provide support to the company. The personnel end state will be a collection of 0688/89s to perform DCO functions, intelligence Marines to provide the necessary threat intelligence and analysis to drive the direction of the defense, and finally, the officer component to advocate and lead the company. The establishment of the DCO-IDM companies and the staffing by the 0688/89s fix a problem that the Marine Corps has faced since the integration of cybersecurity and cyberspace operations into the MAGTF.[28] Figure 2 provides a conceptual framework for the DCO-IDM companies' staffing from a 0688/89 standpoint, with the remaining bodies dedicated to support staff and leadership.

The future of Marine Corps cybersecurity and the responsibilities of this community (0689) are being absorbed by the communications field as a whole.[30] This change has forced the cybersecurity community to develop and morph into a new capability set (0688/89) consisting of DCO.[31] The establishment of the DCO-IDM company provides a location from which these new 0688/89 Marines will be able to operate outside of MARFORCYBER and the cyber protection teams. A paradigm shift in the Marine Corps lies in the reality that with the establishment of these companies, there is not a need within the rest of the Marine Corps units to have organic 0688/89s. The current role of a 0689 is to provide cybersecurity capabilities to the MAGTF, but the new 0688/89 is a DCO-centric Marine who supports advanced defensive capabilities. An option available with the creation of the DCO-IDM companies will be the ability to pull all current 0688/89s from their MAGTF units and consolidate them into a centralized location within the DCO-IDM company.[32] This consolidation scares some, as they believe they are losing a capability, but, in all actuality, they are gaining a resource within the properly trained and equipped DCO cell. Once joined to any exercise or operation through a simple request to the DCO-IDM company via the communications battalions, each MAGTF element will have DCO capabilities. The concept of employment for these companies allows for the attachment of the DCO Marines, similar to a radio battalion team construct, to any exercise or operation and their return to the company to increase the knowledge of the community. By forming a centralized location from which these companies can operate, the MEFs will have the ability to consolidate resources, integrate cyber intelligence collection, and operationalize a cyber capability within all facets of the MAGTF.

The assignment and task organization of these companies is key to their success. Currently, the DCO-IDM companies are an asset assigned to the communications battalions.[33] This may seem like a logical addition to these units, but it also raises concerns for their future mission accomplishment. The biggest concern about this organization is the lack of organic intelligence assets within the communication battalions. DCO relies on threat intelligence to drive and direct follow-on actions. The DCO-IDM company structure requires that every request for information be sent to an external unit and prioritized against its other requests. This is extremely inefficient and does not produce the agile adaptability that the Marine Corps is accustomed to within its operational units. Another concern with the companies attached to the communications battalions is the lack of access to the top-secret networks that house the bulk of the intelligence and information needed to support cyberspace operations. The realm of cyber is one that resides on the top-secret networks; the lack of access organic to the communications battalions creates another inefficiency. This adds to the reason why these units should not reside within the communications battalions. Otherwise, they need access to these networks within each unit.

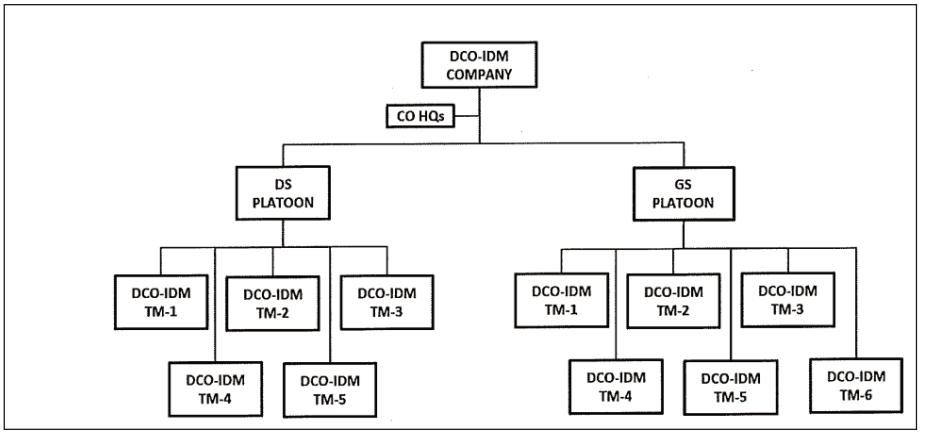


Figure 2. Conceptual depiction of the 0688/89 staffing structure within the DCO-IDM companies.[29]

A radical solution to these problems would be the establishment of not only the DCO-IDM company but a new cyber operations battalion with the DCO-IDM company as a component. The cyber operations battalion would include a company of cyber intelligence collection and analysis Marines and the staff to support, as well as the DCO-IDM company and battalion support structure. The leadership would be comprised of an operations cell that integrates with the G-3 at the MEF for task assignment and completion. This battalion would provide the holistic cyber component to the MEF and allow for future integration of the offensive cyber capabilities. As a MEF information operations asset, the cyber operations battalion would fall under the MIG structure subordinate to the MIG commander. The cyber operations battalion would integrate the intelligence needed to drive a proper defense and the defensive technicians capable of manipulating the environment to ensure the success of the mission, all while supporting cyberspace operations from a MEF and whole MAGTF perspective.

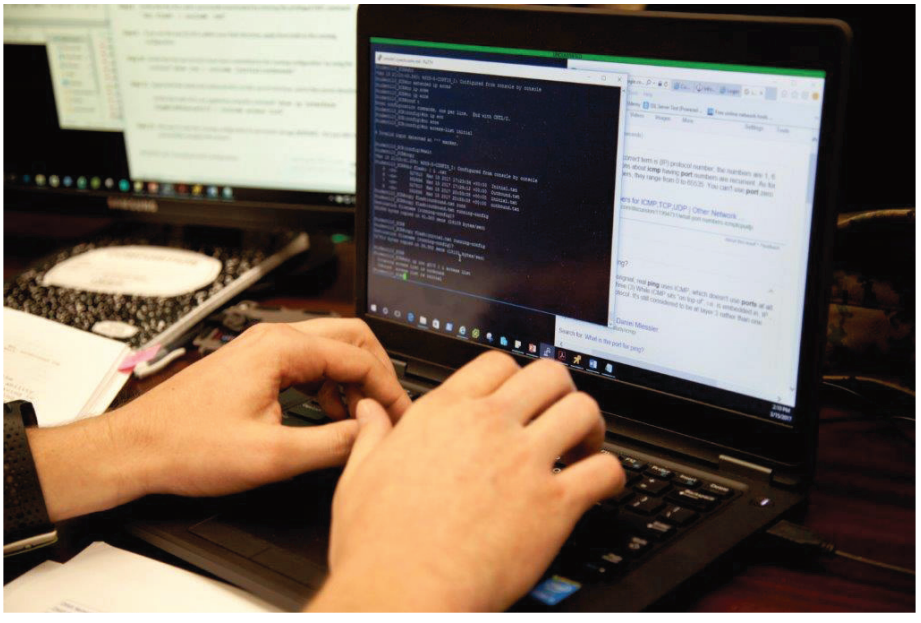
Another alternative for the DCO-IDM company is the initiative proposed by MARFORCYBER that would establish and staff the companies within the MEFs, but they would receive tasks from and report directly to MARFORCYBER. This proposal, while effective from a DCO perspective, does not provide the MEFs with the level of control they would like for an organic unit. This struggle for power and control over the DCO-IDM companies poses a unique problem for the future of this capability and whether the Marine Corps is ready to have this level of cyber down at the tactical edge.

Final Operational Capability

The current state of the DCO-IDM companies makes it difficult to identify the final operational capability. As this capability continues to mature, the future needs of these companies will continue to evolve. Final operational capability marks the end of official evaluation but does not stop the continued adaptation that happens within any Marine Corps unit to increase effectiveness and efficiency. This section focuses on the future employment of these companies and demonstrates the full integration of cyberspace operations into every facet of the MAGTF. As cyber continues to advance, and as the use of cyber becomes more and more ingrained in all aspects of warfare, it is necessary to increase capability and to continue to strive to complete the integration of cyber resources.

Key terrain may be identified through the integration of cyber threat intelligence into Operating Force planning. *(Photo by Cpl Jonathan Sosner.)*

Final operational capability requires the complete staffing of the DCO-IDM companies within the MEFs. The anticipated date of completion for this staffing is circa 2020.[34] This extended period allows for the transition of the 0688/89 MOS into the realm of properly trained DCO technicians/chiefs and ensures that these companies are



The final operational capability of the DCO internal defensive measures has yet to be identified. *(Photo by LCpl Jose VillalobosRocha.)*

staffed with the personnel capable of performing the mission. The creation of these companies allows for a fixed action within the Marine Corps and the 0688/89 MOS by providing an additional unit for these Marines to be stationed in. A significant problem within this MOS is the fact that these Marines are highly trained, skilled, and sought after by civilian and other government agencies. Providing an additional unit allows for diversity within the Marine Corps and the spread of knowledge from the team construct of MARFORCYBER to the new operational capability within the Operating Forces. The DCO capability will become an asset available to all elements of the MAGTF and allow for the future integration of OCO to create the construct of full cyberspace operations to the tactical edge.

Final operational capability for the DCO-IDM companies requires a lot of shifts and ideas that the Marine Corps may or may not have the desire to complete. The appetite exists for this capability, but the shaping of the future and the role of these companies will determine their fate. Integration of the DCO-IDM companies with the MIGs will be a key to success. Regardless of the end state, the building, staffing, and training of DCO-IDM companies is happening already. At least for the near future, they will be a component of the MEF, falling under the MIG. The creation of these companies allows the Marine Corps to continue to lead the DOD in extending cyberspace operations into the lowest possible level.

Conclusion

Each of the sister Services has developed robust training programs in order to establish and maintain their cyber mission forces.[35] The Marine Corps, while also establishing the training, has sought to lean forward and advance past the other Services by establishing cyberspace capabilities outside of the team construct within the cyber mission forces and allowing for the use of this capability within the Operating Forces. As cyber matures within the Marine Corps, the model established through the creation of these DCO-IDM companies will allow for the reuse of this blueprint within the other Services, for further expansion by the Marine Corps into other areas of cyberspace operations, and for the ability to push these capabilities to the lowest unit possible.

The use of DCO within the Marine Corps Operating Forces will increase their ability to defend themselves from adversarial actions in the cyber domain.[36] Though this article only describes the use of one of the two subsets of DCO, the creation of the DCO-IDM companies will allow for the integration of cyber capabilities, cyber threat intelligence, and the operational capacity to provide an active threat defense to the Marine Corps Enterprise Networks. These companies are the initial salvo of cyber capabilities enabled within the Operating Forces and will ensure the future success of the Marine Corps in the arena of cyber, which will continue to be at the forefront of warfare.

Notes

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

2. Ibid.

3. LtGen K.J. Glueck, *MCIP 3-32Ei, Marine Corps Cyberspace Operations*, (Washington, DC: 2016).

4. *Joint Publication 3-12 (R).*

5. *MCIP 3-32Ei.*

6. Headquarters Marine Corps, *MCO 5239.2B, Marines Corps Cybersecurity*, (Washington, DC: 2015).

7. *Joint Publication 3-12 (R).*

8. *MCIP 3-32Ei.*

9. *MCO 5239.2B.*

10. *MCIP 3-32Ei.*

11. *MCO 5239.2B.*

12. *MCIP 3-32Ei.*

13. E.H. Larsen, "MEF DCO-IDM Team Initial Operating Capability Concept."

14. Ibid.

15. Ibid.

16. Ibid.

17. Ibid.

18. Ibid.

19. *MCIP 3-32Ei.*

20. Ibid.

21. A. Carter, *DOD Cyber Strategy*, (Washington, DC: 2015).

22. Department of Defense, *DOD Strategy for Operating in Cyberspace*, (Washington, DC: 2011).

23. *MCIP 3-32Ei.*

24. *DOD Cyber Strategy.*

25. *DOD Strategy for Operating in Cyberspace.*

26. C. Torres, Jr., private communication, February 2017.

27. MSgt W.W. Hess and GySgt R.M. Moore, "Cybersecurity of the Future," *Marine Corps Gazette*, (March 2017).

28. Torres.

29. Torres.

30. "Cybersecurity of the Future."

31. Ibid.

32. Torres.

33. "MEF DCO-IDM Team Initial Operating Capability Concept."

34. Ibid.

35. Department of the Army, *Strategic Cyberspace Operations Guide*, (Carlisle, PA: U.S. Army War College, 2016).

36. *MCIP 3-32Ei.*