Marine Corps Concept for Cyberspace Operations

9 October 2015

Version 2.0

Distribution Statement A
Approved for Public Release

This Page Intentionally Left Blank

TABLE OF CONTENTS

This Page Intentionally Left Blank

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3300 RUSSELL ROAD
QUANTICO, VA 22134-5001

Foreword

Threats within and emanating from cyberspace are among the most significant challenges the Marine Corps faces, and will continue to face, in future operating environments. A growing number of actors working individually, in groups or with state-sponsorship, can potentially disrupt military operations through malicious cyber activity. The low cost of entry, widespread availability of attack vectors, and difficulty of tracing sources of activity, all contribute to the threat proliferation. While these technologies create challenges that present significant risks to the Marine Corps, the same technologies also present opportunities to shape the environment, control escalation and, when necessary, apply force through cyberspace – within a combined arms framework – to overwhelm and defeat adversaries.

The *Marine Corps Concept for Cyberspace Operations* addresses the cyberspace capabilities the Marine Corps will need to support missions as part of a joint force and meet requirements of the Combatant Commanders. It stresses that commanders must integrate cyberspace capabilities into the operational plans across the warfighting functions and domains, and shows that integration and synchronization of cyberspace and electromagnetic spectrum operations will be critical to mission success.

In developing strategies and capabilities for operating in cyberspace, commanders and force developers must focus on the central aspects of the cyber threat, especially those that affect Marine Corps operational abilities. This concept details that the Marine Corps must address cyberspace vulnerabilities and underscores the importance of continuous training and education to overcome the difficulties of operating in a degraded or denied cyberspace environment. It stresses the need for a professional, Service-retained cyberspace workforce to support operations and defense of the Marine Corps Enterprise Network and, when directed, conduct offensive cyberspace operations.

This concept intends to inform and guide the Marine Corps Capabilities Based Assessment process by identifying the cyberspace operations capabilities the Marine Corps will require to achieve the vision described in *Expeditionary Force 21 Forward and Ready: Now and in the Future*. Force developers can further define these required capabilities, identify gaps, and recommend and implement solutions using a doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy methodology. This concept addresses and applies to Headquarters Marine Corps and all elements and command echelons of the supporting establishment and operating forces.

Robert S. Walsh

ROBERT S. WALSH
Lieutenant General, U.S. Marine Corps
Deputy Commandant, Combat Development and Integration

This Page Intentionally Left Blank

1 Introduction

The *Marine Corps Concept for Cyberspace Operations* describes the capabilities the Marine Corps needs to conduct cyberspace operations as a function of its combined arms capability to support the mission requirements of Combatant Commanders (CCDRs). It aims to inform the Marine Corps Capabilities Based Assessment process so that force developers can identify gaps and recommend appropriate doctrine, organization, training, materiel, leadership and education, personnel, facilities and policy (DOTMLPF-P) solutions that will enable the Marine Corps to conduct globally integrated operations as part of a joint force.

This concept covers the timeframe from 2017-2025 and applies to Headquarters Marine Corps and all elements and command echelons of the supporting establishment and operating forces. It addresses requirements for the three missions of cyberspace operations: Department of Defense information networks (DODIN) operations, defensive cyberspace operations (DCO) and offensive cyberspace operations (OCO) across the range of military operations (ROMO)[1]. This concept is based on Joint and Service guidance and concepts, and directly supports the central ideas in the Marine Corps capstone concept *Expeditionary Force 21 Forward and Ready: Now and in the Future.*

This document reflects the strategic, operational, and tactical considerations for employing and equipping Marine air-ground task forces (MAGTFs) and the supporting establishment (SE) to support operations across the ROMO. It focuses deliberation on the MAGTF's ability to operate in complex environments characterized by growth of social media, availability of information technology (IT), importance of signature[2] management, challenges to electromagnetic spectrum (EMS) access and the globalization of cyberspace capabilities.[3] This concept outlines the need to extend and protect critical expeditionary enterprise services such as voice, video, data and collaboration across the globe to support operations in all environments and extend power projection capabilities across all domains.

2 Future Operating Environment[4]

Since 2013, the Director of National Intelligence has ranked cyberspace threats first among the strategic threats to the United States, surpassing terrorism.[5] Hostile actors will use cyberspace operations as an asymmetric capability to strike key U.S. government and private sector functions and services, directly and indirectly. Globally important critical infrastructure is vulnerable to cyberspace attacks, placing economic systems and military missions at risk. Some state and non-state actors will attack Department of Defense networks in an effort to disrupt command and control to

[1] Joint Publication 3-12 (R)

[2] "A signature is the characteristic of an indicator that makes it identifiable or causes it to stand out…Reducing the uniqueness or stability of the indicator's signature increases the ambiguity of the adversary's observations." MCO 3070.2A, The Marine Corps Operations Security (OPSEC) Program, 2 July 2013. p. 3-1.

[3] Expeditionary Force 21 Forward and Ready: Now and in the Future, 4 March 2014, p. 13.

[4] Extracted from Expeditionary Force 21, pp. 9-11.

[5] The DOD Cyber Strategy, 17 April 2015, p. 9.

adversely affect the U.S. military's ability to mobilize in the event of a contingency.[6] Adversaries could then amplify first order effects through propaganda and information operations to generate cascading risks to force and mission.

These new challenges in cyberspace and the EMS[7] mean the U.S. military can no longer presume to hold the information advantage. Opponents will use a combination of advanced networked information systems and innovative, cost-effective tactics to degrade, disrupt, deny, and/or destroy Marine Corps processes and systems. Advancements in commercial technologies and adversary offensive capabilities increase the operational complexity in the cyberspace domain. The exploitation of cyberspace threatens U.S. military global command and control. Accordingly, naval forces must have the resilience to operate under the most hostile cyberspace conditions[8], as well as the expertise to continue utilization of the domain for operational benefit.

These cyberspace threats add another dimension to the volatility, instability and complexity that will frame the security landscape. Current intelligence estimates indicate that national and international challenges will stretch the employment capacity of the U.S. military. This operating environment will demand a force in readiness with capabilities for a global response. Weapons proliferation and increased cyberspace capabilities among a broader range of state and non-state entities is likely to continue.

Many of these challenges and opportunities will occur in the littorals; those congested and diverse areas where the sea and land merge. Most maritime activities—commercial shipping, fishing, and oil and gas extraction, for example—take place within 200 miles of the shore. Additionally, more than 80% of the world's population currently resides within 100 miles of a coastline—and the percentage is increasing. In many cases, threats to U.S. interests may require expanding the concept of littoral maneuver hundreds of miles inland. Geography and demographics are creating a future security environment with a significant littoral dimension; one in which an "Arc of Instability" that encompasses the littorals of South Central Asia, the Middle East, Africa and Central and South America, is prominent.

Naval forces, because of their readiness, responsiveness, flexibility, precision and strategic mobility, are essential to ensuring continued access and security in the global commons and the littorals. The once likely need to conduct sustained operations ashore has decreased, and it is more probable that over the next 10 years naval forces will need to address small-scale crises and limited contingencies in and around the littorals. It is increasingly likely that major operations and campaigns, should they occur, will transpire in the maritime domain and the littorals.

[6] Mission Analysis for Cyber Operations of Department of Defense, 21 August 2014, p. 6.

[7] "The cyberspace domain and the EMS are interrelated "maneuver" spaces through which military advantage can be either gained or lost. Cyberspace can only be leveraged for maximum tactical advantage when EMS-dependent capabilities are combined with cyberspace operations capabilities to support MAGTF operations." MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept, 1 May 2014, p. 1.

[8] A Cooperative Strategy for 21st Century Seapower, March 2015, p. 8.

The Marine Corps must use the sea and advanced bases to “turn the anti-access/area-denial (A2/AD) table” on an adversary, either prior to or in the midst of a conflict. Likewise, the ability to establish a series of numerous austere advanced bases—by occupation or seizure—as a means of dispersing aircraft, missiles, and intelligence, surveillance, and reconnaissance assets may become an imperative. Establishing—or merely demonstrating the ability to establish—such “oceanic outposts” would strengthen the Marine Corps’ ability to reassure allies and deter adversaries.

The increased range, precision, and proliferation of A2/AD systems highlight the need to conduct dispersed operations with smaller, task-organized forces. CCDRs are increasing their demand for tailored forces to conduct theater security cooperation activities with a wider number of partner nations. Theater commanders must also be prepared to quickly consolidate and reorganize forces into larger formations to expeditiously deal with escalating crises and contingencies. These demands call for a new approach to how we organize, deploy, employ and sustain forces—especially with regard to effectively linking Marine Corps, Navy, Coast Guard, Special Operations Command and partner capabilities, to include the integrity and governance of information systems. Accordingly, the Marine Corps must revise its methodology toward capability and capacity development, especially given the rapidly evolving technologies and the unpredictable vulnerabilities they may present.

The Marine Corps of the future will operate in an increasingly contested cyberspace operational environment. Success of future operations hinges on development of robust technologies and flexible tactics, techniques and procedures. The rapid expansion of social media enables social and identity-based movements to cross geographic boundaries. These same technologies empower individuals to be destructive across both cyberspace and physical domains by enabling adversaries to stage indirect attacks throughout the buildup, deployment, and sustainment phases of US military operations. Cyberspace operations bring an entirely new dimension to warfare. Accordingly, the Marine Corps must prepare to operate in environments where it will be constantly subject to exploitation and attack in the cyberspace domain via vectors that include the Internet. Commanders should expect that adversaries will exploit unprotected information systems, and networks with poor security. Cyber-attacks do not necessarily require substantial investments in technology, only a cunning and capable opponent.

3 Military Challenge

Cyberspace is a global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[9] To fully adapt to the operational imperatives and opportunities in cyberspace, the Marine Corps must increase its capability and capacity to operate in and exploit the cyberspace domain.[10]

[9] Joint Publication 1-02, p. 58.

[10] U.S. Marine Corps 36th Commandant’s Planning Guidance, 26 February 2015, p. 11.

All warfighting functions are increasingly dependent upon freedom of action in cyberspace. The data, processing capacity, and connectivity required to enable timely decision-making and a rich communications environment requires robust cyberspace operations capabilities. Both MAGTF commanders and our adversaries have become reliant on these capabilities to increase the speed of their decision cycles. Therefore, MAGTFs require the ability to establish and maintain freedom of action in cyberspace while denying the same to adversaries.

It is unlikely that adversaries will simply cede freedom of action in cyberspace to the United States. They will continuously probe networks and systems during steady state periods, and will likely relentlessly attack them during periods of hostilities. Accordingly, the Marine Corps must protect its data and networks and improve the ability to detect, contain, and respond to such intrusions. However, given the nature of warfare, we can expect that a thinking and determined enemy will persistently exploit and resist, so the Marine Corps must take an added step beyond emphasizing prevention, defense, and recovery. Commanders and staffs must continually train and prepare to operate effectively despite adversarial action—be it known or unknown—within our perimeter. Plainly, commanders and cyberspace operations experts must be able to quickly adapt to adversarial presence inside Marine Corps cyberspace systems.

The Marine Corps' reliance on network-enabled capabilities to collect, process, store, and disseminate information makes the systems susceptible to cyberspace and electronic warfare threats. Accordingly, the Marine Corps must acquire and employ increasingly resilient networks and systems in order to remain operationally effective during network failure, degradation, or significant compromise. Use of redundant systems and physical protection measures can contribute to defense of a network by isolating and neutralizing the impact of obstructions. These solutions, however, are not always economically feasible.

As the Marine Corps seeks solutions to these challenges, force developers must keep in mind four critical considerations when developing cyberspace operations capabilities and the workforce:

- Activities and operations in the cyberspace domain impact objectives within all warfighting domains (land, maritime, air, and space). Success or failure of operations within the cyberspace domain will directly affect the MAGTF's ability to accomplish these objectives.
- The Marine Corps must identify, plan for, and manage operational dependencies, vulnerabilities, and opportunities that arise in and through cyberspace.
- Integrating and synchronizing cyberspace and EMS operations will be critical to MAGTF mission success.
- The need for a rigorously trained cyberspace workforce, a cadre of skilled professionals who can defend Marine Corps systems and offer commanders non-kinetic options to create desired effects against an adversary.

4 Central and Supporting Ideas

In order for the Marine Corps to contribute fully to globally integrated operations and to acquire and maintain all domain access[11], it must possess organic full spectrum (DODIN, DCO, and OCO) cyberspace operations capabilities that deliver desired effects and seamlessly augment the joint force. Globally integrated operations demand a far greater ability to see, understand, operate in and defend cyberspace.[12]

Future joint operations will require forces that are globally postured, can combine quickly with each other and mission partners to integrate capabilities across domains, echelons, geographic boundaries, and organizational affiliations. MAGTF commanders must have the ability to command, control, and coordinate such an interdependent force in rapidly changing scenarios involving distributed, simultaneous, or sequential operations often with other agencies and nations. The rapid, assured exchange of information in this future environment is crucial to the success of MAGTF operations.

Emerging cyberspace threats demand new approaches to managing information, securing information systems, and ensuring the ability to operate through an attack. Increased efficiencies in intelligence-sharing, collaborative-planning, and synchronizing and monitoring execution of operations underscore the need to act and react at machine, not human, speeds.[13] Commanders must approach operations in cyberspace with a new mindset to ensure agile adaptation to challenges, and openly embrace new capabilities to mitigate the threats. Speed of action in cyberspace demands real-time situational awareness. Systems must provide autonomous detection and response capabilities. Marine Corps autonomous devices must, in turn, have protection from adversarial action.

Cyberspace operations will play a more prominent role in future missions. Accordingly, planners must integrate cyberspace operations capabilities at the lowest echelons—not just at the higher headquarters—to make them a viable and reliable military option.[14] MAGTF commanders must consider and employ cyberspace operations as a supporting arm in addition to being an enabler. Doing so will expand the MAGTF's combat power and increase the effectiveness of other capabilities. When fully integrated across domains and echelons, cyberspace operations will enhance the MAGTF's global responsiveness, strategic flexibility, and operational effectiveness.

Incorporating these capabilities into the operational design will increase the mission's probability of success. Integrating and coordinating cyberspace operations into the intelligence, planning and targeting process will promote the combined arms effect to maximize advantage over an adversary. Cyberspace operations capabilities enable maneuver warfare, allowing commanders freedom of action to impart effects at the time and place of their choosing. As the information residing within the cyberspace domain grows, so too will the demand for intelligence capabilities used to exploit this information in support of commanders' decision-making.

[11] "All domain access is the ability to project military force in contested areas with sufficient freedom of action to operate effectively." A Cooperative Strategy for 21st Century Seapower, March 2015, p. 19

[12] CJCS Joint Information Environment White Paper, 22 Jan 2013, p. 4.

[13] 2010 Joint Operating Environment, 18 February 2010, p. 36.

[14] Joint Concept for Cyberspace Operations, Version 1.7, 21 May 2015, p. 8.

A commander's freedom of action presupposes access to all network and communications resources required to accomplish the assigned mission and the authority to direct operations. The cyberspace domain allows effects to cross functions, domains, and boundaries instantly and could have widespread consequences beyond the operational environment. The currently overlapping authorities required for approval of cyber effects further complicate cyberspace operations. Often, the fleeting opportunities in cyberspace require immediate decisive action. MAGTF commanders require the ability to execute cyberspace operations and produce effects at a time and place of their choosing. The existing process should not undermine the commander's ability to impart cyberspace operations effects when they deem it necessary. Synchronizing cyberspace operations with activities in other domains and lines of operation will enable commanders to gain and sustain advantages across the ROMO. Planners must orchestrate DODIN operations, DCO and OCO through frameworks that arrange time, space and purpose so they can lead to timely and appropriate action. It is imperative that the integration of functions and the approval process preserves the tenet that enables action by a single commander. Responsive cyberspace operations require a clear and efficient approval process.[15]

When executed with appropriate permissions and de-confliction measures, the effects generated by the MAGTF's organic OCO capabilities will be contained within the MAGTF's area of operations. Such capabilities must be able to support the missions of higher headquarters, as directed. This will ensure MAGTF commanders have broad array of possible effects and capabilities at their disposal, and streamline the coordination necessary to employ them. Targeting and intelligence capabilities that support OCO demand a high level of precision and timing. A MAGTF's ability to conduct OCO will be limited by the availability of organic and non-organic targeting and intelligence resources.

DCO requires threat monitoring, detection, analysis, and response actions. DCO also requires greater understanding of the operational environment through finding, mitigating, and fixing cyber-related threats and vulnerabilities. DCO systems must give commanders proper indications and warning to enable a selection of the appropriate course of action. Intelligence capabilities that support DCO must first focus on the collection and identification of activities, which occur outside of friendly networks. This intelligence will inform decision-making and internal defensive measures taken within Marine Corps networks. It is important to differentiate between those defensive systems that monitor networks' health, and the intelligence capabilities that focus on collection and identification of external threats not yet introduced to Marine Corps networks. In all cases, the architecture supporting these networks must be seamless, leaving no exploitable gaps. It is likely that the Marine Corps will never achieve a perfect defense against adversarial action in cyberspace, especially since adversaries can co-opt our offensive capabilities and replicate their effects against Marine Corps systems.

The Marine Corps' reliance on information networks to enable timely decision-making in support of operations creates a vulnerability we must mitigate. As the Marine Corps matures the tactics, techniques, and procedures required to support a persistent

[15] Ibid., p. 12.

information network, it must continue to explore and rehearse methods to maintain combat effectiveness in a communications degraded environment. Networks must incorporate resiliency characteristics that will support the continued operation of key functions while defensive cyberspace measures are implemented, and provide appropriate protection of information without undue sacrifice of functionality. A persistent information network is essential for MAGTF operations.

The vision of the Marine Corps Information Enterprise (MCIENT) Strategy is to "provide a secure, scalable, adaptive, and flexible Marine Corps Information Environment that supports operations across a broad spectrum of missions in order to ensure access to the right data, at the right place, at the right time."[16] The strategy presents a conceptual model, with the Marine Corps Enterprise Network (MCEN) at its core, for the Marine Corps Information Environment, consistent with the DODIN and the future Joint Information Environment (JIE). The MCEN must be capable of extending its services to the tactical edge under any condition. It must be flexible enough to adapt to technology and network demands, enforce cybersecurity standards, mitigate threats, repel attacks, and enable seamless access across the enterprise. Achieving this posture requires standardizing the staffing, training and equipping of the MAGTF Data Centers.

Unlike other domains with fixed physical features, cyberspace continues to evolve and grow in complexity. Marine Corps training and the MAGTF's ability to operate in and maneuver through this domain must be equally evolutionary. Operations within this domain will require a highly trained cyberspace workforce. Marines, government service civilians, and contractors must have the technical and analytical skills to employ advanced encryption methods, detect anomalies, identify vulnerabilities and otherwise leverage the capabilities of the JIE in order to support network operations.

Recruiting, training, and maintaining a professional cyberspace workforce requires significant coordination between Marine Corps Recruiting Command, Manpower and Reserve Affairs, Training and Education Command, Occupation Field Managers, and others. This coordination will provide an integrated resource that Manpower and Reserves Affairs carefully manages with a dedicated focus on continued training and education to meet emerging technical developments. These personnel will be indispensable in assisting commanders to achieve MAGTF and joint objectives. A well-trained cyberspace workforce will ensure and enhance Marine Corps capabilities across all domains, provide cyberspace operations options for commanders, and defend against adversary actions within cyberspace.

To this end, as cyberspace operations capabilities evolve and gaps in current and programed cyberspace operations training and education are identified, the Marine Corps will update current individual and collective training and education or develop new training and education to mitigate or close the identified gaps. Expanded education will enable Marines to accept and understand that cyberspace operations are non-lethal options that produce asymmetric yields and increase mission success rates. Ultimately, commanders need a trained workforce that is sufficiently agile, flexible, fast, adaptable, and skillful to function and prevail in a dynamic environment.

[16] Marine Corps Information Enterprise (MCIENT) Strategy 2015-2020 (Draft), p. 6.

A solid doctrinal foundation reinforced by continuous training and education is imperative to exploit opportunities and operate successfully in a degraded/denied cyberspace environment. Accordingly, in addition to formal education, Marines must conduct training events and tactical exercises to simulate operations in a degraded cyberspace environment during all phases of mission execution. Scenarios must present a variety of missions, threats, and conditions that vary dynamically to test the agility of C2 and cyberspace operations capabilities. Unit performance and mission readiness will improve when exercises focus on completing unit mission essential tasks with degraded access to network resources.

To maximize the workforce's capability, the Marine Corps must properly align it to operational requirements. We must leverage the Department of Defense initiative that has established a Cyber Mission Force whose focus will be on individual CCDR and Service requirements. Trained Marines will contribute to the Cyber Mission Force that will support CCDRs in carrying out approved operational plans and contingency operations with integrated cyber effects.[17] These Marines must be skilled and qualified to meet the needs of both the CCDR and the Service in the areas of DODIN operations, DCO and OCO.[18]

Cyberspace operations support all operations, and its artful employment may ultimately determine the level of mission success. OCO requires deliberate coordination and integration to ensure desired effects. DODIN operations and DCO must be sufficiently robust and network redundancies must be agile and stratified to provide security and continued availability despite an adversary's attempts to exploit or attack critical systems and networks. Potential adversaries have significant cyberspace capabilities to disrupt and degrade MAGTF operations. Accordingly, commanders and their staffs must prepare and train for operations in a satellite denied or degraded environment, a constrained bandwidth environment, as well as operations with locally available data and networks until connectivity can be restored.

5 Required Capabilities

To achieve DODIN, DCO, and OCO advantages, for both MAGTF and joint cyberspace operations, the Marine Corps must acquire and integrate the right balance of advanced technology and cyberspace capabilities, employ a responsive command and control structure with a streamlined approval process, issue clear guidance and policies, implement a comprehensive legal framework, and field a well-trained and mission-ready workforce. Accordingly, the Marine Corps will require the following cyberspace operations capabilities:

Department of Defense information networks (DODIN) operations

DODIN operations are operations to design, build, configure, secure, operate, maintain, and sustain Department of Defense networks to create and preserve information assurance on the Department of Defense information networks.[19] These networks are the globally interconnected, end-to-end set of information capabilities,

[17] Joint Concept for Cyberspace, Version 1.5, 27 March 2015, p. 9.

[18] Ibid.

[19] Joint Publication 3-12 (R), Cyberspace Operations, 5 February 2013, p. GL-4.

and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security.[20] The Marine Corps Network Operations and Security Center is responsible for the operation and defense of the MCEN which provides the Marine Corps portion of the DODIN. The Marine Corps must have the ability to:

- Effectively command and control the MCEN via a singular, centralized commander with clear authorities and C2 structure.
- Deliver end-to-end enterprise IT transport services.
- Provide flexible, rapidly deployable, scalable, and joint interoperable IT services.
- Enable a secure and highly available information environment to support C2 of the MAGTF and continuum of information extended from garrison to the operating environment.
- Provide interoperable and transportable enterprise communications for Service, joint, combined, interagency and non-governmental organizations to support the full range of military operations.
- Collect system demand history and usage rates in an automated and real-time manner.
- Operate networks in a degraded, contested, compromised, or locally denied cyberspace environment.
- Enable isolated portions of the network to continue to operate autonomously.
- Provide standard and automated configuration management.
- Plan, engineer, install, operate, and interconnect reliable, assured, scalable, and modular networks.
- Monitor the health and status of the network and information systems in an automated and real-time manner.
- Provide situational awareness regarding information system resources and the network.
- Conduct preventive system maintenance on network resources in an entirely automated and real-time manner.
- Ensure only accredited systems connect to the network.
- Conduct unified and/or federated identity and access management.
- Prevent intrusions.
- Operate interoperable networks across security domains.

Defensive cyberspace operations (DCO)

These are passive and active cyberspace operations intended to preserve the ability to utilize friendly cyberspace capabilities and protect data, networks, net-centric capabilities, and other designated systems.[21] To conduct DCO effectively, the Marine Corps needs the ability to forecast, detect, identify, and respond to adversarial actions against the MCEN and the information resident in its networks. Responses to unauthorized or malicious cyberspace activity will require commanders to dynamically

[20] JP 1-02.

[21] Ibid.

reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised networks to ensure continuous access to specific portions of cyberspace. Accordingly, the Marine Corps requires the ability to:

- Provide organic intelligence support to DODIN operations and DCO.
- Detect and respond to intrusions throughout the MCEN.
- Protect from intrusions throughout the MCEN.
- Perform defensive cyberspace operations internal defense measures[22] to mitigate risk from a known or perceived threat.

Offensive cyberspace operations (OCO)

These are cyberspace operations intended to project power by the application of force in or through cyberspace.[23] Commanders require the ability to target adversary systems and related capabilities in and through cyberspace in support of mission accomplishment. OCO requires deliberate coordination and integration to ensure desired effects. Accordingly, the Marine Corps, at all MAGTF levels, requires the capability to:

- Integrate organic and non-organic OCO-related capabilities with actions in all domains in support of the MAGTF mission.
- Conduct ISR within the cyberspace domain.
- Provide intelligence support to OCO.
- Conduct OCO when required.
- Conduct battle damage assessment of cyberspace fires.

General capabilities

General capabilities are capabilities that support all three cyberspace operations mission areas.

- Rapidly acquire, develop, test and deploy secure solutions to emerging and legacy technical challenges.

6 Risks

There are some potential risks associated with adopting the ideas proposed in this concept. While some require an exclusive technical solution, commanders can mitigate these risks through consistent training and education. To realize the vision and ideas in this concept, it is incumbent on commanders, leaders, and force developers at all levels to devise and implement strategies to manage the following risks:

Inadequate integration of cyberspace operations into operational plans.

This may result in MAGTFs not achieving the full effects of combined arms or benefiting from the cross-domain effects cyberspace operations can achieve.

[22] "Defensive Cyber – Internal Defense Measures are the ability to dynamically reestablish, re-secure, reroute, reconstitute, or isolate degraded or compromised local networks ensuring sufficient cyberspace access for joint forces." Joint Capability Areas Lexicon, 9 January 2015, paragraph 6.1.4.

[23] JP 1-02.

Commanders can mitigate this through education and training to ensure staff and planners understand the value of integrating cyberspace operations capabilities into operations.

Insufficient resilience in systems.

Fiscal drivers and competing demands may limit investments in redundancy/ resiliency yet commanders will still be required to operate in degraded environments.

The Marine Corps can mitigate this risk through proper investments and allocation of resources and personnel, in addition to training and education on operating in degraded environments. Building cyber resiliency will require Service/agency/ COCOM coordination to establish the appropriate breadth and depth of stratified capabilities and delineate authorities. Resiliency will facilitate deterrence as it assures continuity of operations.

Acquisition process is inadequate to timely develop, field, and sustain cyberspace operations capabilities and training systems.

Timely system updates and refreshes are a vital element of MAGTF cyber success. Failure to rapidly acquire emerging technology and co-evolve organizational and doctrinal innovation may lead to inefficiencies in the deployment and utilization of cyberspace operations systems and concepts. Such failure may result from unresponsive acquisition processes, insufficient technological advancement, or inability to keep pace with developing counter technology.

The Marine Corps can mitigate this risk by streamlining the requirements process, improving combat development management, and continuing reform of the defense acquisition process.

Increased dependence on information processes, systems, and technologies.

This risk adds potential vulnerabilities that adversaries could exploit if systems are not adequately defended.

The Marine Corps can mitigate this risk through increased and focused network security training and emphasis at all levels and the development of new Information Assurance strategies and technologies.

Over-reliance on information and communications technologies.

This may result in forces becoming incapable of operating effectively in the absence of those technologies, if the technologies fail or are degraded.

The Marine Corps can mitigate this risk by improving resiliency of new technologies, providing adequate levels of redundancy in system architectures, and ensuring that basic functions can be accomplished with minimal or no reliance on information and communications systems. Formal learning centers can integrate degraded, contested, compromised, or denied cyberspace environment training into conditions for 2000-level Training and Readiness events and awareness training into 1000-level Training and Readiness events. Additionally, commanders can conduct training and exercises that realistically simulate conditions of MCEN failure and attack.

7 Conclusion

The Marine Corps' reliance on cyberspace makes it vitally important that MAGTFs, Headquarters, and the supporting establishment possess the capabilities and expertise necessary to leverage operational advantage through this domain. These capabilities will increase a MAGTF commander's ability to apply force through cyberspace, protect networks, enable real time attack prevention and detection; make possible attack response through event identification and actions such as deception, blocking and/or denying; and allow the coordination of appropriate counterattacks. Simply, MAGTFs must be properly organized, trained, and equipped to conduct cyberspace operations at the time and place of the commander's choosing. These operations must be integrated and synchronized throughout all warfighting functions to realize the vision of the Marine Corps' capstone concept, *Expeditionary Force 21, Forward and Ready: Now and in the Future*.

Force developers must consider these central and supporting ideas, required capabilities and risks during follow-on capabilities-based development efforts to develop appropriate DOTMLPF-P solutions.

Appendix A - References

Guidance

Quadrennial Defense Review 2014, 4 March 2014

The National Military Strategy of the United States 2015

U.S. Marine Corps 36th Commandant's Planning Guidance, 26 February 2015

U.S. Marine Corps Service Campaign Plan 2014-2022, 20 June 2014

Concepts

A Cooperative Strategy for 21st Century Seapower, March 2015

Capstone Concept for Joint Operations Activity Concepts, Version 1.0, 8 November 2010

Capstone Concept for Joint Operations: Joint Force 2020, 10 September 2012

Expeditionary Force 21 Forward and Ready: Now and in the Future, 4 March 2014

Expeditionary Force 21, Marine Expeditionary Brigade Concept of Operations, Forward and Ready: Now and in the Future, 11 July 2014

Joint Concept for Cyberspace, Version 1.7, 21 May 2015 (Draft)

Joint Concept for Entry Operations, 7 April 2014

Joint Operational Access Concept, Version 1.0, 17 January 2012

MAGTF Cyberspace and Electronic Warfare Coordination Cell (CEWCC) Concept, May 2014

Marine Corps Operating Concept for Information Operations, 4 February 2013

Naval Operations Concept 2010, 27 April 2010

Doctrine

Joint Publication 3-12(R), Cyberspace Operations, 5 February 2013

Joint Publication 3-13, Information Operations, November 2012

Marine Corps Doctrinal Publication 1, Warfighting, 20 June 1997

Marine Corps Doctrinal Publication 1-0, Marine Corps Operations, 9 August 2011

Marine Corps Interim Publication 3-40.02, Marine Corps Cyberspace Operations, 6 October 2014

Other

CJCS Joint Information Environment White Paper, 22 January 2013

Defense Information Systems Agency Strategic Plan 2015-2020

DOD Cyber Strategy, 17 April 2015

Expeditionary Warrior 2014 Final Report, 16 July 2014

Marine Corps Information Enterprise (MCIENT) Strategy 2015-2020, 10 April 2015

Marine Corps Order 3100.4, Cyberspace Operations, 27 July 2013

Marine Corps POM-18 JCA 5 and 6 CBA Database (Secret), accessed April 2015

Mission Analysis for Cyber Operations of Department of Defense, 21 August 2014

Secretary of Defense Memorandum – Designation of Offices of Primary Responsibility for the Lines of Effort and Objectives in the DOD Cyber Strategy, 19 June 2015

2015-2025 Future Operating Environment, Implications for the Marine Corps (Secret//REL to USA FVEY), August 2015

This Page Intentionally Left Blank