

NOT FOR PUBLICATION UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS &
CAPABILITIES

STATEMENT OF

LIEUTENANT GENERAL RICHARD P. MILLS
DEPUTY COMMANDANT
COMBAT DEVELOPMENT AND INTEGRATION &
COMMANDING GENERAL, MARINE CORPS COMBAT DEVELOPMENT COMMAND

BEFORE THE

HOUSE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

CONCERNING

DIGITAL WARRIOR: IMPROVING MILITARY CAPABILITIES
IN THE CYBER DOMAIN

ON

July 25, 2012

NOT FOR PUBLICATION
UNTIL RELEASED BY
THE HOUSE ARMED SERVICES COMMITTEE
SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

Introduction

Chairman Thornberry, Ranking Member Langevin, and distinguished members of this Subcommittee, it is an honor to appear before you today. On behalf of all Marines and their families, I thank you for your continued support. We value what this Committee is doing to highlight the importance of cyberspace operations; and the Marine Corps appreciates your support as we collaborate with the other Services to develop our cyber capabilities and workforce capacity to support Department of Defense policies, U.S. Cyber Command requirements, and integrate cyber across the Marine Air Ground Task Force (MAGTF). While we are making great progress, we recognize that the risks are increasing daily.

As the nation's expeditionary force in readiness, the Marine Corps is prepared for all manner of crises and contingencies – including those arising in the cyber domain. We recognize the complex, highly adaptive threats that we face. In the future, as in the past, multiple regional powers and a host of lethal groups will exploit numerous seeds of instability, proliferating increasingly lethal technology and extremist ideology, while leveraging the advantages of networks hidden amongst the population. Marines are prepared to meet these challenges with our Navy, Special Operations, Army, Air Force and interagency partners.

New strategic guidance issued by the President and the Secretary of Defense provides the framework by which the Marine Corps will balance the demands of the future security environment with the realities of our current budget. The guidance calls for a future force that is “agile, flexible, and ready for the full range of contingencies. In particular, we will continue to invest in the capabilities critical to future success, including intelligence, surveillance, and reconnaissance; counterterrorism; countering weapons of mass destruction; operating in anti-access environments; and prevailing in all domains, including cyber.”¹ Operating effectively in cyberspace is now a primary mission of the U.S. Armed Forces. The guidance re-validates the Marine Corps' role as America's expeditionary force in readiness – forward deployed and forward engaged, ready to manage all manner of crises and contingencies.

In this evolving strategic security environment, the Marine Corps recognizes that it cannot conduct operations without reliable information, communications networks, and assured access to cyberspace. Ensuring a stable cyber domain means ensuring stability for our weapons systems, command and control, industrial assets, et al. The cyber domain touches every aspect of our operations and must be contemplated at the lowest levels in the Marine Corps planning process. Indeed, Marines have been conducting cyber operations for more than a decade, and we are in a multi-year effort to expand our capacity. Three years ago, the Marine Corps established U.S. Marine Corps Forces Cyber Command (MARFORCYBER). We have made great strides in expanding the capability and capacity of MARFORCYBER, as well as our cyber-related Military Occupational Specialties. We plan to increase our cyber workforce by approximately 700 Marines and Civilian Marines through FY16. Given the fiscally constrained environment and complexity of cyberspace, our approach is focused on increasing capacity for network operations, defensive cyberspace operations, and when directed, offensive cyberspace operations; and through the introduction of planners within our command element staffs to further integrate cyberspace operations into our plans and operations.

¹ *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, January 2012, White House letter.

Overview

The rapidly evolving events of the past year alone indicate a new constant. Competition for resources; natural disasters; social unrest; *hostile cyber activity*; violent extremism; regional conflict; proliferation of weapons of mass destruction; and advanced weaponry in the hands of the irresponsible are becoming all too common. Marine Corps intelligence estimates rightfully point out that “more than half of the world’s population live in fragile states, vulnerable to ruinous economic, ideological, and environmental stresses. In these unstable regions, ever-present local instability and crises will erupt, prompting U.S. responses in the form of humanitarian assistance and disaster relief operations, actions to curtail piracy, stability operations, and the rescue and evacuation of U.S. citizens and diplomats.”²

In this unpredictable, unstable and uncertain future security environment, there is an emphatic trend in warfare--the dynamic combination of conventional and irregular warfare by state, non-state and criminal threats. The Marine Corps is manned, trained and equipped to continuously adapt to, deter and defeat these adversaries with increasingly discriminating and precise full spectrum operations. Through a comprehensive force structure review, we designed a post-Operation Enduring Freedom force in readiness that counters this hybrid threat, creates options and provides decision space for senior leadership while, when necessary, setting the conditions for a comprehensive joint, interagency and allied response.

As we look to the future, the post-Operation Enduring Freedom Marine Corps of 182,100 is fundamentally different from the current and pre-9/11 force. It draws on a rich history of innovations in irregular warfare but is recast as a scalable crisis response force ready to counter complex irregular, conventional and hybrid threats--and the gray areas in between. We have substantially invested in relevant organizations such as Marine Special Operations; intelligence, surveillance and reconnaissance; communications; partnering; civil affairs; electronic warfare; regionally oriented command and control; information operations; and of increasing importance - cyberspace operations. Task organized with our highly trained line units, these enablers provide versatile, scalable capability for a broad range of missions to include deterrence, counter-terrorism, counter-proliferation, partnering, reinforcement to our allies, humanitarian assistance, and assured access for the joint force under any condition our national interests require.

The Marine Corps will conduct full spectrum cyberspace operations - to include Department of Defense information network operations, defensive cyberspace operations, and when directed, offensive cyberspace operations - in support of Marine Corps Operating Forces, the supporting establishment, the joint force, and combined operational requirements, in order to enable freedom of action across all warfighting domains while denying the same to adversaries. Recent cyber accreditations and readiness inspections validate our network operations command and control processes and procedures. As we transition to a Government owned and operated network environment, the Marine Corps will pursue efficiencies through automation, consolidation and standardization to ensure availability, reliability and security of cyber assets. The Marine Corps has already standardized its security boundary architecture and its implementation on the Marine Corps Enterprise Network (MCEN) and is working with the Joint

² *Five Year Forecast: 2012-2017 Assessment of International Challenges and Opportunities That May Affect Marine Expeditionary Forces* January 2012, pg 1.

Information Environment framework to comply with the developing shared security architecture standards. As we assume full control over our network transport and enterprise services, we will collapse remaining legacy networks which reduce our management footprint and costs, while achieving greater compliancy and consistency throughout the MCEN. Underlying all these efforts has been a consistent process development, improvement and enforcement of our Enterprise IT Service Management plan whereby we maintain strict control over network changes while still providing communication and information system services to all users in all mission areas.

In the sections below we describe the strategic, operational and tactical importance of cyberspace operations for the Marine Corps; how we will meet future demands for supporting Marine Air Ground Task Force (MAGTF) operations; and our vision for ensuring a stable network that is secure, robust and yet flexible enough to support the Marine Corps' role as America's expeditionary force in readiness.

Current Developments

Cyber Work Force

The Marine Corps Force Structure Review positions the Marine Corps to respond to the most likely missions while preserving the capability to project punishing combat power when required. The cornerstone of the future Marine Corps rests on the quality and flexibility of our Marines, which allow us to support the joint force commanders' diverse requirements. Our 182,100 Marine Corps represents fewer infantry battalions, artillery battalions, fixed-wing aviation squadrons, and general support combat logistics battalions than we had prior to 9/11. However, it adds cyber operations capability, Marine special operators, wartime enablers and higher unit manning levels—all lessons gleaned from 10 years of combat operations; it is a very capable force.

Cyberspace operations play an essential role in addressing future operations. The future force will include enhanced cyber capabilities enabled by:

- Reorganizing our intelligence collection and exploitation capabilities to enhance readiness by directly linking deployed forces, garrison support, and the intelligence community; and
- Increasing capacity for full-spectrum cyber operations by increasing structure across appropriate MAGTF and Supporting Establishment units/organizations, and by increasing the structure of Marine Corps Forces Cyber Command.

The development of Marine Corps cyber forces is progressing on schedule, with all forces scheduled to be fully manned by FY16.

Organizations/Units

MARFORCYBER provides cyber capabilities through its subordinate elements: the Marine Corps Network Operations and Security Center (MCNOSC) and Lima Company, Marine Cryptologic Support Battalion (Lima Company). Together, these units operate, maintain, and defend the Marine Corps Enterprise Network; conduct defensive cyber operations as part of its routine operations as well as offensive cyber operations when directed.

Network Architecture

The Marine Corps Systems Command is the Engineering Competency provider for the Marine Corps with the systems engineering expertise across all engineering disciplines - including computer, networking and cyber security to deliver secure tactical and enterprise systems. The Marine Corps Cyber Engineering strategy takes a holistic, enterprise-wide view and is focused on an end-to-end security architecture. The network architecture strategy focuses on designing systems securely from the beginning - during systems engineering development. By ensuring that network defenders understand the network's design, we increase the ability to protect the network.

The Marine Corps has made significant progress in reducing the number of applications across the functional areas.

The Marine Corps Enterprise Network consists of network infrastructure and equipment, and the people and processes that work on and within the network - from forward deployed tactical users, bases and air stations, to Headquarters Marine Corps staff. As we transition from the Navy Marine Corps Intranet network to a Government Owned, Government Operated network, we are implementing enterprise network management processes with associated tools that will permit our Marine Corps Network Operations and Security Center, our Regional Network Operations and Security Centers, and our Marine Air Ground Task Force IT Support Centers to operate and defend the network and provide services in an enterprise construct, while still regionalizing the network for optimal local support and local control during emergencies or crises. Our Next Generation Enterprise Network contract will provide the necessary support for us to achieve full regionalization and ultimately Marine Corps Enterprise Network unification. Our Marine Corps Enterprise IT Services provides enterprise-wide application hosting with the Marine Air Ground Task Force IT Support Centers hosting regional and local applications to better support users. We are currently assessing whether our enterprise-level Marine Corps Enterprise IT Services data center will be designated as a DOD Enterprise Core Data Center so that other DOD users and the Joint Information Environment can leverage it.

The Marine Corps will participate fully in the Joint Information Environment while retaining our service unique capabilities and maintaining control of the Marine Corps Enterprise Network down to the desktop. As Joint Information Environment enterprise services are developed, tested, certified, and accredited for use, we will assess their applicability to our mission and adopt those services that meet our requirements.

Current and Future Capability

The Marine Corps recently conducted a comprehensive Cyberspace Operations Capability Based Assessment (CBA) across all lines of operation (Department of Defense Information Network Operations, Defensive Cyber Operations and Offensive Cyber Operations) to determine our requirements for the full spectrum of cyberspace operations. The Marine Corps Cyberspace Operations Initial Capabilities Document (ICD) prioritizes non-materiel and materiel Doctrine, Organization, Training, Materiel, Leadership, Personnel, Facilities and Policy solutions to address identified cyber capability gaps. We are now initiating actions to close these gaps and update the USMC Cyberspace Operations Concept.

Conclusion

We are taking a deliberate and joint approach to cyber requirements; and we continually strive for the right balance in supporting the requirements of U.S. Cyber Command and our Service requirements. We work closely with U.S. Cyber Command to build the necessary mission capabilities, and we will adjust our approach as we learn more about the challenges and opportunities ahead. With the support of the Congress and the American people we can ensure the Marine Corps, along with the other Service components and U.S. Cyber Command, is ready for the current fight and is well prepared to secure our Nation and national interests in an uncertain future. Again, I thank you for the opportunity to discuss cyberspace operations.