NOT FOR PUBLICATION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

STATEMENT BY

MAJOR GENERAL DANIEL J. O'DONOHUE
COMMANDING GENERAL
MARINE FORCES CYBERSPACE COMMAND

BEFORE THE

SENATE ARMED SERVICES COMMITTEE

SUBCOMMITTEE ON EMERGING THREATS AND CAPABILITIES

MILITARY CYBER PROGRAMS AND POSTURE

FIRST SESSION 114TH CONGRESS

April 14, 2015

NOT FOR PUBLICATION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

Major General Daniel J. O'Donohue

Major General O'Donohue graduated from the College of William and Mary with a Bachelor of Arts in History and was commissioned in 1984.

Command assignments include: Commanding Officer, Charlie Company, 1st Battalion, 2nd Marines (1993-1995), Commanding Officer, 2nd Battalion, 5th Marines (2002-2004), Commanding Officer, 1st Marine Regiment (2009-2010), Commander, Marine Corps Forces Cyberspace Command (2015).

Staff assignments include: Ground Structure Planner, Headquarters Marine Corps (1988-1992); 8th Marines Operations Officer (1995-1996); Operations Officer, Joint Task Force Assured Response and Special Purpose Marine Air-Ground Task Force Liberia (1996); Tactics Instructor and Expeditionary Operations Program Director, Amphibious Warfare School (1997-2000); Operations Officer, 1st Marine Division (2001-2002); Assistant Chief of Staff G-7 / Division Combat Assessment Officer (2004); Deputy Branch Head, Secretary of the Defense's Office of Force Transformation (2005-2007); Branch Head, Ground Combat Element Branch, Plans, Policies and Operations, Headquarters Marine Corps (2007-2008); Assistant Chief of Staff G-3, 1st Marine Division (2008-2009); Director, Capabilities Development Directorate, Headquarters Marine Corps (2010-2012); Deputy Director for Force Management, Joint Staff J-8 (2013), Deputy Chief of Staff for Operations, ISAF Joint Command (2014).

He is a distinguished graduate of the Naval Postgraduate School, Amphibious Warfare School, School of Advanced Warfighting, and National War College. He has Masters of Science Degrees in Management and National Security Strategy.

He is married to the former Kathleen ("Rani") Pinch and they have seven children.

Introduction

Chairman Fischer, Ranking Member Nelson, and distinguished members of this subcommittee, it is an honor to appear before you today. On behalf of all Marines, our civilian workforce, and their families, I thank you for your continued support. I appreciate the opportunity to discuss the Marine Corps' cyberspace operations posture.

The Marine Corps is the nation's expeditionary force-in-readiness. We are forward deployed, forward engaged, and prepared for crisis response. For generations, your Marines have been victorious against our nation's foes by remaining agile and adaptable to dynamic environments and evolving threats. As the force that is 'the most ready when the nation is least ready,' we are prepared to defend against adversaries who operate across multiple domains to include cyberspace.

Our current operating environment is volatile, complex, and distinguished by increasingly sophisticated threats that seek asymmetric advantage through cyberspace. Our cyberspace posture guards against these threats, while simultaneously exploiting our competitive advantage in employing combined arms to include closely integrated cyberspace operations.

Our joint cyberspace mission builds on the Marine Corps institutional focus as a global crisis response force with strong naval, inter-agency, COCOM, SOF, cross-service and coalition partnerships. 2015 is a key transitional year as we deploy rapidly maturing cyber capabilities and make them central to Marine Air Ground Task Force, COCOM and coalition training, planning and operations. Activities in cyberspace increasingly influence all our warfighting functions.

Marine Forces Cyberspace Command (MARFORCYBER) is engaging in ongoing cyberspace operations, making strong progress with the force build, achieving operational outcomes, and building capacity for tomorrow's opportunities and challenges. Our priorities are to operate and defend our networks, support designated COCOMs with full spectrum cyber operations, organize for the fight, train and equip the cyber workforce, develop workforce

lifecycle management, and to ensure mission readiness through joint and service capabilities integration.

Mission and Organization

As the service component to U.S. Cyber Command, MARFORCYBER conducts full spectrum Cyberspace Operations to ensure freedom of action in and through cyberspace, and deny the same to our adversaries. The operations include operating and defending the Marine Corps Enterprise Network (MCEN), conducting Defensive Cyberspace Operations (DCO) within the MCEN and Department of Defense Information Networks (DODIN), and - when directed - conducting Offensive Cyberspace Operations (OCO) in support of Joint and Coalition Forces. MARFORCYBER is also designated at the Joint Force Headquarters – Cyber (JFHQ – CYBER) as directed by USCYBERCOM.

The Marine Corps is in a period of transition from multiple legacy contractor owned and operated networks to a unified system architecture that is organized according to our warfighting philosophy and doctrine. We are building a Naval approach that will enable the warfighting functions for competitive advantage in a complex environment. These unique characteristics give our service a competitive advantage in an intersecting battlespace.

Operationalizing Cyber

MARFORCYBER is in its sixth year of operation. Our focus remains developing ready cyberspace capability for the naval, joint and coalition force. Consistent with our Commandant's guidance, we are developing tactical cyber capacity as an organic aspect of how we fight. Marines will increasingly operate and defend in a compromised and degraded environment. We must align our operational readiness standards and risk mitigation to this reality. Our battlefield networks must be resilient, redundant and interoperable, and extend from the garrison environment forward to the tactical edge of battle.

Further, in conjunction with joint and interagency partners, we intend to pursue the development of an integrated and unified platform for cyberspace operations that will enable

centralized command and control, real time situational awareness, and decision support. We are accomplishing this through close coordination with industry partners, and aligned with DoD and USCYBERCOM priorities in support of the Joint Information Environment.

Train and Equip

In this presumably automated and system driven arena, our most valuable resource is our people. Just as the Marine Corps remains dedicated to the notion that there is no more dangerous weapon than a Marine and his rifle, we must provide our Marines with the tools and resources they need to defend our nation. In order to maintain an asymmetric advantage, we must outpace our adversaries' ability to develop and procure those resources. The acquisition process by which we acquire vehicles and aircraft incurs steep opportunity costs when applied to cyber technology and innovation. Our acquisition processes are deliberately procedure heavy and risk averse, to ensure appropriate delivery of viable solutions. Statutory and regulatory changes will be required in order to enable responsiveness to emerging cyber threats and missions. Current acquisition processes do not adequately support the delivery tempo required for emerging cyber solutions. The tempo at which emerging technologies must be acquired to meet cyberspace operational mandates is occurring at a much greater pace, which creates tension within the acquisition process. We must strike a balance between rapid acquisition to meet emerging threats and changing operational demands and maintaining disciplined engineering rigor of enterprise networks. Adaptability and flexibility are critical to ensuring our cyber mission force teams are ready.

MARFORCYBER's approach to training and developing the cyber work force has a singular vision—to train as we fight. Specifically, MARFORCYBER will adapt a persistent training environment to support training and exercises of cyber units that are assigned to conduct military cyber operations. This training environment will be designed to enhance military occupational skills (MOS) proficiency, test and development of next generation solutions, host remote training and education of Marine Corps Operating Forces, and refine tactics, techniques, and procedures (TTPs) to increase effectiveness of cyberspace operations.

Additionally, we are developing a web based training environment hosted by Carnegie Mellon University Software Engineering Institute (CMU-SEI), a Federally Funded Research and Development Center (FFRDC). This environment combines extensive research and innovative technology to offer a new solution to cyberspace operations workforce development. The focus of this collaboration is to help practitioners and their teams build knowledge, skills, and experience in a continuous cycle of professional development. The combined effect of this approach is for cyberspace operations workforce to train individually and collectively. This initiative will support the future development and certification of Cyber National Mission Forces (CNMF) training requirements.

We have dramatically increased cyber integration into the training cycle by leading, supporting, or participating in over 31 combined, joint, and Marine Corps exercises in the past year. Commanders across our Marine Corps are asking for cyber capabilities both in real world operations and in training to ensure their Marines are ready to face the challenges presented by a shifting complex landscape.

Workforce Life-Cycle Management

We have seen substantial increases in capacity and capability. Such achievements are significant but they have not been easy, and MARFORCYBER's success grows from the hard work of its people. Marines and Civilians have shown a sharp interest in pursuing a cyber career.

Since 2012, we have dramatically increased our workforce—with an authorized strength of almost 1000 Marines and civil servants today. By the end of fiscal year 2016, MARFORCYBER's authorized strength will increase to over 1300 personnel, which is in line with previous projections. The majority of these new personnel are allocated to support the cyber mission force as directed by the Secretary of Defense.

In order to attract and retain the best people, the Marine Corps has followed multiple lines of effort. To improve continuity and reap greater return-on-investment in the lowest density highest demand military occupational specialties (MOS), we have coordinated with our

Service to extend standard assignments to four years. Additionally, the number of feeder MOS available to lateral move into critical cyber related specialties has been increased in order to obtain a larger talent pool of qualified and experienced Marines. We are currently accessing sixteen feeder occupational specialties from the communications, signals intelligence, electronic warfare, data, and aviation specialty fields to meet the personnel demands of cyber occupational field. The largest reenlistment or lateral move bonus offered in the past year of $60,750 dollars was offered to Sergeants who move into the Cyber Security Technician specialty. To drive home the point of how seriously the Marine Corps takes its cyber talent management, this bonus consumed 16% of the retention bonus budget for the last fiscal year. Furthermore, to ensure we have the right metrics, we are leveraging academia and industry to understand how to better attract and retain talent. In the future, our focus will broaden to include generating a sustainable force generation model that retains a unique, skilled expertise within the larger contexts of cyber ready MAGTFs.

Going forward, the Marine Corps is reviewing its manpower models, and considering new management structures to adapt with the increasingly complex and technical aspects of the security environment in which we operate. Beyond technical training, we will place an increasing emphasis on leaders with experience to shape and mentor incoming talent. Courses of action are being developed today in order to impact our manpower models this summer. In the long term, we will look forward to your assistance in order to re-shape this new paradigm.

Readiness

MARFORCYBER is leading the effort to take cyberspace operations mainstream across the Marine Corps so as not to be outpaced in an evolving and complex battlespace. Initial teams are being operationally employed as they achieve IOC. As we support the DoD and USCYBERCOM efforts to implement a unified cyberspace architecture of the JIE, we continue to improve the operational readiness of our existing enterprise network (MCEN). We have assumed full control of the MCEN, which was previously contractor-managed, and have decreased our legacy network footprint.

In conjunction with joint, interagency, and private partners, we intend to improve our operational readiness and our ability to measure it. In this context, our staff is working and collaborating with our partners to develop rapid acquisition of tools, training environment, and development of procedures that will allow us to train as we fight.

Last June, USCYBERCOM certified our first Cyber Mission Team (CMT) as fully operational (FOC) and simultaneously, our first national Cyber Protection Team (CPT) and the second Cyber Mission Team (CMT) reached initial operational capability (IOC). MARFORCYBER is on track to have over 75% of its CMT, CPT, and CST teams resourced by the end of fiscal year 2015.

In order to fulfill the requirements of USCYBERCOM, we have been actively engaged in building and sourcing our national and combat mission, protection, and support teams (CMT, CPT, CST). With one CMT currently certified, the plan going forward is to have MARFORCYBER's second CMT certified early in calendar year 2015. We have one operational CPT working from the MCNOSC, which is our service wide network operations and security center. Our second CPT, which will be in support of national missions, is in the process of certification now. In addition, we stood up our Joint Forces Headquarters-Cyber (JFHQ-C), now at Full Operational Capability (FOC), which directs and coordinates the actions of cyber forces in support of directed missions. The current glide slope for team build-out is to have two (2) CMTs, three (3) CPTs, and one (1) CST at either IOC or FOC by the end of fiscal year 2015. No later than the end of FY17 all teams will be FOC, meaning the Marine Corps will furnish one (1) NMT, three (3) CMTs with one (1) CST in support, and eight (8) CPTs. Three of those CPTs will be dedicated to Marine Corps' specific needs. All other teams will function in support of joint requirements from unified and sub-unified combatant commands.

Conclusion

Over the past six years, MARFORCYBER experienced both the increased risk and opportunity presented by a world that grows more connected. These experiences reinforced the need to remain focused on our priorities of developing our organization and cyber work

force, refining our service support to MAGTF operations and joint cyber forces, and securing our networks to yield results for commanders worldwide. Although I am pleased to report that our growth is increasing our capacity, capability, and integration with warfighters, I must reiterate the opportunities and challenges that lie ahead are great. While global technology advances rapidly, the Marine Corps faces challenges in adapting its acquisitions to operate at the speed required of cyberspace. Critically, in this domain characterized by human activity, people remain our center of gravity. Resourcing and sustaining this most valuable asset also remains a difficult task. These are difficult challenges, but through your continued support and leadership, we can count such difficulties among the many that Marines have overcome in the defense of this great nation.

Thank you for this opportunity to appear before you today. Thank you for your continued support of our Marines and Civilians and I look forward to answering your questions.