

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE
ARMED SERVICES COMMITTEE

STATEMENT OF
VADM MICHAEL S. ROGERS
COMMANDER, UNITED STATES FLEET CYBER COMMAND
BEFORE THE
EMERGING THREATS AND CAPABILITIES
OF THE
HOUSE ARMED SERVICES COMMITTEE
ON
25 JULY 2012

NOT FOR PUBLICATION UNTIL
RELEASED BY THE
HOUSE
ARMED SERVICES COMMITTEE

Chairman Thornberry, Ranking Member Langevin and distinguished members of the Subcommittee, thank you for the support of our military. I appreciate the opportunity to appear before you today with my counterparts from the other military services and to discuss the United States Fleet Cyber Command and U.S. TENTH Fleet.

Mr. Chairman, I have been in command of U.S. Fleet Cyber Command and U.S. Navy TENTH Fleet for just under a year. As the Navy's Component Command to United States Cyber Command, and an Echelon Two Command, subordinate to the Chief of Naval Operations, Fleet Cyber Command directs cyberspace operations in defense and support of Navy and Joint forces to deter and defeat aggression while ensuring freedom of action. Since my predecessor, VADM Barry McCullough, testified before this Subcommittee last September, the Department of Defense and the Navy continue to mature cyberspace operations by growing the workforce, exercising our process, and developing the capabilities that support those operations. This progress is, and continues to be, guided by the *DOD Strategy for Operating in Cyberspace*. I would like to take this opportunity to highlight a few areas of progress over the past year and some of the challenges that we continue to address.

Operations

The Department of Defense and the Navy have made significant strides in our ability to conduct cyberspace operations. It has been an iterative process and we will continue to refine our concepts and doctrine as necessary, but there are two major achievements that I would like to bring to your attention. First is the Transitional Command and Control Concept of Operations which was approved by the Secretary of Defense this past May. This CONOPS provides geographic Combatant Commanders and the Services a standard baseline for executing cyberspace operations by documenting Joint Cyber Center and Cyber Support Element command

relationships, missions, functions, and tasks. It also serves as a common starting point for assessing and refining cyber command and control in the future. For its part, the Navy is working closely with U.S. Cyber Command and the other Services to implement and assess this transitional command and control framework. The second item that I would like to highlight is the initial U.S. Cyber Command Operational Directive 12-001 that was issued to each of the Service Component Commands this past April. This Operational Directive specifies standard tasks and mission responsibilities for each of the Service Components, providing initial insight into how U.S. Cyber Command intends to use the Service Components in the planning and execution of cyberspace operations. This in turn, provides a foundation for generating Navy planning and resource requirements. Both of these efforts provided much-needed initial guidance and the Navy will continue to support U.S. Cyber Command and collaborate with the other Service Component Commands to continually assess and refine lines of effort as cyberspace operations evolve.

The Navy's support to Joint and Navy exercises is a critical element to our continual improvement of cyberspace operations. These exercises provide an invaluable opportunity to test our capabilities and identify areas of improvement across the six military functions of Command and Control, Intelligence, Fires, Movement and Maneuver, Sustainment, and Protection. U.S. Pacific Command's Terminal Fury 2012 is one such example that allowed us to exercise cyberspace operations as part of a larger joint operation. The lessons learned from this exercise, and those like it, directly inform the development and refinement of doctrine and tactics, techniques, and procedures. In addition to Joint exercises, U.S. Fleet Cyber Command conducted war games and tabletop exercises to continue to refine Service-level tactics, techniques, and procedures. However, as my predecessor has stated, cyberspace is a man-made

domain and is continually changing. We cannot rest on our past success or recent progress; we must continually exercise and refine our cyberspace operations to keep pace with the evolving threat. Moreover, building and sustaining a highly capable cyber workforce is critical to our operations. Navy initiatives, such as the ongoing Cyber Wholeness Review, will define areas of concern so the Department of the Navy can align resources efficiently to the challenges identified in the cyber domain.

Additionally, the Navy continues to take steps to strengthen our cyber capability afloat through aggressive cyber inspection programs, assist visits, and the use of Navy evaluation teams. Prior to deployment, Navy afloat commands and cyber systems are groomed and assessed for compliance with Department of Defense information assurance requirements. These systems and their operators are evaluated at-sea by Navy teams who further probe cyber systems using tactics, techniques and procedures that potential threats may employ against our forces. This ultimately results in increased cyber readiness across the maritime domain to address the ever changing cyber environment.

Workforce

The Navy's workforce is perhaps our greatest strength in this emerging discipline. Our Sailors and civilians are at the forefront of advances in cyberspace operations for the past several years in the Navy and Joint community. However, the recruitment, development, and retention of a highly capable cyber workforce remain a significant challenge, given the rapidly evolving nature of cyberspace and the intense competition from industry for top talent. Over the past year, the Navy has made significant strides establishing the necessary policy, incentives, and training to recruit, develop, and retain a highly capable cyber workforce.

We have several efforts underway to enhance recruitment of individuals with critical cyber warfare skill sets by building awareness of Navy cyberspace operations and associated career options. The U.S. Naval Academy established a summer intern program with the Navy Cyber Warfare Development Group, enabling midshipmen to gain exposure to a wide range of cyber activities over a six week period as part of their summer training. A similar program was established for Naval Reserve Officer Training Corps midshipmen with computer-related curriculums that allow them to attend the Navy Cyberspace Defense Operations Command for their First Class summer cruise. Additionally, the Navy established the Cyber Warfare Engineer career field enabling direct accessions for a few recent college graduates each year with deep cyber-expertise. These Cyber Warfare Engineers will apply the principles and techniques of computer science and computer engineering to research, design, develop, test, and evaluate software and firmware for computer network attack, exploitation, and defense in cyberspace operations. Our biggest roadblock to maintaining a highly skilled workforce is competition with industry as well as other government agencies demand signal for technical experts. While the Navy cannot compete with the compensation offered by industry, we provide individuals with unique opportunities that they cannot receive out in industry and the highly motivated Navy cyber workforce is opting to stay Navy at record levels. Building awareness of those opportunities early on is central to our recruiting efforts.

Developing and maintaining cyber expertise is another critical focus area for the Navy and the broader Department of Defense. To meet the Operational Commanders' requirements we need a training model that has the ability to rapidly adapt to external innovations and evolving threats. We have supported Department of Defense, U.S. Cyber Command, and Department of the Navy efforts to establish the necessary standards for professional development

and continuous learning that provide the foundation for an effective training model. We incorporated these standards into the implementation of a tiered cyber training strategy for the Navy workforce that tailors cyber training based on an individual's roles and responsibilities. The first tier focuses on building cyber awareness across all users on cyber threats and the role of cyberspace in naval operations. The second tier is tailored towards leadership and focuses on their responsibilities for Navy networks and building accountability for the application of offensive and defensive cyber capabilities. The third tier is designed to build a professional cyber workforce, ensuring they develop and maintain the expertise necessary to conduct effective cyberspace operations across the full range of military operations. As part of this strategy the Navy is implementing an adaptive end-to-end approach that includes both formal and informal training throughout one's career. We will employ a flexible training delivery model that includes traditional schoolhouse training that will be augmented with training through a virtual environment. This will enable our Sailors and civilians to stay up to date on the latest threats and technology advances while mitigating cost and the loss of key personnel from units for an extended period of time. In addition, The Navy Cyber Manpower 2020 Task Force has been established to plan and execute the steps necessary to develop a comprehensive near to mid-term cyber manpower strategy based on the results of the recently completed Navy Cyber Manpower Zero Based Review (ZBR), validated operational requirements and a properly aligned and focused Navy force posture that is supported by a prioritized POM resourcing submission across the Future Year Defense Plan (FYDP). This workforce effort will be in phases and include defensive and offensive cyber operations for all officers, enlisted and civilians. It will include partners in industry and other agencies and will reflect a new force balance of organic

and situational alliances. The final phase will address the workforce focused on cyber capabilities embedded in warfighting systems.

Strengthening our Networks

To reduce the attack surface exposed to criminals and our adversaries, the Navy engaged in a comprehensive campaign to achieve shore network consolidation and modernization by terminating all Navy legacy networks by 2014. This is being accomplished either by consolidating those networks and applications into a standard Navy Enterprise Solution or by terminating the capability as being no longer needed. Since early 2007, over 1000 Navy shore-based networks have been terminated, and those allowed to remain are being brought under strict standards for security and operations under the central command and control of US Fleet Cyber Command. This improves our aggregate security posture, streamlining our network command and control, and delivers cost efficiencies.

The Navy has emphasized cross-communication between our large network programs, Next Generation Enterprise Network (ashore) and the Consolidated Afloat Networks and Enterprise Services (afloat). Common standards and architecture will deliver a consistent operational environment that works to reduce inefficiencies in operations, training, maintenance, and life cycle support costs that come from specialized, one of a kind, technical solutions. Because networks are closely linked with our combat systems, synchronization of new capabilities must be worked in great detail across all the Navy's Systems Commands.

The Navy is also actively engaged in the developing concepts of a Joint Information Environment which will be comprised of information technology infrastructure and enterprise services. This effort is expected to improve mission effectiveness, increase security, and realize IT efficiencies across the Department of Defense. Over the past year we have supported multiple

pilot efforts that will help shape and inform the development of the Joint Information Environment. Additionally, the progress we have made in developing the Next Generation Enterprise Network and the Consolidated Afloat Network Enterprise Services informed the development of the Joint Information Environment. This includes Navy's efforts in network consolidation, identity management and access control, data center consolidation and enterprise services. As we continue to move forward, we will ensure that the Navy's efforts remain aligned and supportive of the Joint Information Environment.

The investments we have made in network consolidation and deployment of enterprise services have already provided the Navy with greater situational awareness of our networks. This includes near-term insight into the health of our networks as well as long-term trend analysis of attack, sensing, and warning data to detect more discrete cyber threats and irregularities. For example, The Navy's Computer Network Defense Service Provider has just completed development of a capability to allow operators to visualize enterprise level data to identify trends specific to a region or area of operations. The Navy's improvements in cyber situational awareness have begun to improve the efficiency and effectiveness of our operations and enabled us to provide U.S. Cyber Command with a more complete picture of Navy Networks.

In addition to network consolidation and enhancing situational awareness, the Navy continues to make strides in enhancing our network defense capabilities, particularly in our tactical environment at sea. A critical component of this effort was the deployment, operation and maintenance of the Host Based Security System, or HBSS. The Navy has significant challenges in terms of the sheer number of HBSS servers that it must deploy in order to account for every shore and afloat unit. Despite this challenge the Navy achieved 100% deployment of

HBSS across the SIPRNET enclave and is in the process of deploying HBSS across the NIPRNET afloat enclave.

While we have made significant progress enhancing our networks and their defense, we must remain agile. Over the past year U.S. Fleet Cyber Command substantially broadened its efforts to identify Navy network vulnerabilities. We assumed ownership for the U.S. Cyber Command inspection program for Navy sites, added an emphasis on personnel network behavior, and doubled the number of Navy sites inspected compared to previous years.

In many cases it is difficult to determine if an open vulnerability could lead to an exploit with negative mission impact. We generally assume that a dedicated adversary would be capable of exploiting open vulnerabilities. We also assume that a clever adversary would wait to use this capability until it would provide a tactical or strategic advantage. The difficulty of trying to determine if an adversary knows about a vulnerability, is capable of exploiting it, and has the will to do so, has led us to focus on a zero-tolerance methodology.

Our biggest challenge is determining which vulnerabilities equate to a credible risk to mission. We find few sites fully compliant, and yet we find few sites that have been compromised or are at serious risk of compromise. The challenge lies in being able to link non-compliance with operational risk. As we move forward, we will continue to refine our inspection methodology to provide greater insight into which vulnerabilities have the potential to have a substantially negative impact on mission accomplishment, and which would have little to no effect if exploited, allowing the Navy to focus limited resources on the most critical areas.

Summary

Our success in the maritime domain and joint operational environment depends on our ability to maintain freedom of maneuver and deliver effects within cyberspace, and to

accomplish this, the Navy's workforce needs to be highly trained and possess the skills required to operate in this ever changing environment. To ensure we maintain our edge the Navy will continue to drive advancements in Navy cyberspace operations, and will be guided by the *Department of Defense Strategy for Operating in Cyberspace*. This strategy, combined with the CNO directed Cyber Wholeness Review, scheduled for the late summer; demonstrates the Navy's commitment to Cyber Operations. I believe, based on the ever increasing requirements and diversity of the threat, that it is safe to assume our cost will increase no matter how efficient we become in this domain. I thank you for this opportunity to present the efforts of U.S. Fleet Cyber Command and U.S. TENTH Fleet, and appreciate your support of our Navy and Department of Defense. I look forward to answering your questions.