





A Review of the U.S. Navy Cyber Defense Capabilities: Abbreviated Version of a Classified Report

ISBN
978-0-309-36767-7

12 pages
8.5 x 11
2015

Committee for a Review of U.S. Navy Cyber Defense Capabilities; Naval Studies Board; Division on Engineering and Physical Sciences; National Research Council

 [More information](#)

 [Find similar titles](#)

 [Share this PDF](#)



Visit the National Academies Press online and register for...

- ✓ Instant access to free PDF downloads of titles from the
 - NATIONAL ACADEMY OF SCIENCES
 - NATIONAL ACADEMY OF ENGINEERING
 - INSTITUTE OF MEDICINE
 - NATIONAL RESEARCH COUNCIL
- ✓ 10% off print titles
- ✓ Custom notification of new releases in your field of interest
- ✓ Special offers and discounts

Distribution, posting, or copying of this PDF is strictly prohibited without written permission of the National Academies Press. Unless otherwise indicated, all materials in this PDF are copyrighted by the National Academy of Sciences. Request reprint permission for this book

A Review of U.S. Navy Cyber Defense Capabilities:

Abbreviated Version of a Classified Report

Committee for A Review of U.S. Navy Cyber Defense Capabilities
Naval Studies Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

COMMITTEE FOR A REVIEW OF U.S. NAVY CYBER DEFENSE CAPABILITIES

JAMES R. GOSLER, Albuquerque, New Mexico, *Co-Chair*
MIRIAM E. JOHN, Livermore, California, *Co-Chair*
DONNA M. GREGG, Applied Physics Laboratory, Johns Hopkins University
ROBERT L. GROSSMAN, Open Data Group and University of Chicago
BARRY M. HOROWITZ, University of Virginia
RICHARD J. IVANETICH, Institute for Defense Analyses
TERRY P. LEWIS, Raytheon Company
STEVEN B. LIPNER, Microsoft Corporation
ARTHUR L. MONEY, Alexandria, Virginia
FRED B. SCHNEIDER, Cornell University
PAUL A. SCHNEIDER, Annapolis, Maryland
WILLIAM O. STUDEMAN, ADM, USN (Ret.), Severna Park, Maryland

Staff

CHARLES F. DRAPER, Director, Naval Studies Board, Study Director
LYNETTE MILLET, Associate Director, Computer Science and Telecommunications Board
RAYMOND S. WIDMAYER, Senior Program Officer
MARY G. GORDON, Information Officer
MARTA V. HERNANDEZ, Associate Program Officer
SUSAN G. CAMPBELL, Administrative Coordinator

NAVAL STUDIES BOARD

MIRIAM E. JOHN, Livermore, California, *Chair*
CHARLES R. CUSHING, C.R. Cushing & Co., Inc.
JAMES N. EAGLE, Naval Postgraduate School
GEORGE J. FLYNN, Alexandria, Virginia
ROCHEL GELMAN, Rutgers, The State University of New Jersey
JAMES R. GOSLER, Albuquerque, New Mexico
SUSAN HACKWOOD, California Council on Science and Technology
CHARLES E. HARPER, Semtech Corporation
TAMARA E. JERNIGAN, Lawrence Livermore National Laboratory
BERNADETTE JOHNSON, Lincoln Laboratory, Massachusetts Institute of Technology
TERRY P. LEWIS, Raytheon Company
RONALD R. LUMAN, Applied Physics Laboratory, Johns Hopkins University
RICHARD S. MULLER, University of California at Berkeley
JOSEPH PEDLOSKY, Woods Hole, Massachusetts
DAVID P. PEKOSKE, Potomac, Maryland
J. PAUL REASON, Washington, D.C.
ALTON D. ROMIG, JR., Lockheed Martin Aeronautics Company
FRED B. SCHNEIDER, Cornell University
PAUL A. SCHNEIDER, The Chertoff Group
ALLAN STEINHARDT, Booz Allen Hamilton, Inc.
TIMOTHY M. SWAGER, Massachusetts Institute of Technology
RICK D. WEST, Poulsbo, Washington

Navy Liaisons

RADM HERMAN A. SHELANSKI, USN, Director, Assessment Division, Office of the Chief
of Naval Operations, N81
RADM MATTHEW L. KLUNDER, USN, Chief of Naval Research/Director, Innovation,
Technology Requirements, and Test & Evaluation, N84

Marine Corps Liaison

LtGen KENNETH J. GLUECK, JR., USMC, Commanding General, Marine Corps Combat
Development Command

Staff

CHARLES F. DRAPER, Director

CHERIE M. CHAUVIN, Senior Program Officer (as of October 4, 2014)

RAYMOND S. WIDMAYER, Senior Program Officer

MARTA V. HERNANDEZ, Associate Program Officer

SUSAN G. CAMPBELL, Administrative Coordinator

MARY G. GORDON, Information Officer

Abbreviated Version of a Classified Report

At the request of the Chief of Naval Operations, the National Research Council (NRC) appointed an expert committee to review the U.S. Navy's cyber defense capabilities. The Department of the Navy has determined that the final report prepared by the committee is classified in its entirety under Executive Order 13526 and therefore cannot be made available to the public. This abbreviated report provides background information on the full report and the committee that prepared it.

Copies of the report will be made available to authorized individuals in the government from the NRC's Naval Studies Board (<http://sites.nationalacademies.org/DEPS/nsb/index.htm>). Other requests for the report should be submitted to the Department of the Navy.

The project that is the subject of this report was approved by the Governing Board of the NRC, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The members of the committee responsible for the report were chosen for their special competences and with regard for appropriate balance. The study was supported by a contracting arrangement (ref. N00014-10-G-0589-0009) between the National Academy of Sciences and the Department of the Navy.

BACKGROUND

The 2014 Quadrennial Defense Review (QDR), conducted internally by the Department of Defense (DoD) to identify military capabilities that would contribute to fulfilling U.S. national security needs, stated the following:

“The United States has come to depend on cyberspace to communicate in new ways, to make and store wealth, to deliver essential services, and to perform national security functions. The importance of cyberspace to the American way of life – and to the Nation’s security – makes cyberspace an attractive target for those seeking to challenge our security and economic order. Cyberspace will continue to feature increasing opportunities but also constant conflict and competition – with vulnerabilities continually being created with changes in hardware, software, network configurations, and patterns of human use. Cyber threats come from a diverse range of countries, organizations, and individuals whose activities are posing increasingly significant risks to U.S. national interests. Some threats seek to undercut the Department’s near- and long-term military effectiveness by gaining unauthorized access to Department of Defense and industry networks and infrastructure on a routine basis. Further, potential adversaries are actively probing critical infrastructure throughout the United States and in partner countries, which could inflict significant damage to the global economy and create or exacerbate instability in the security environment.”¹

The QDR builds on the former Secretary of Defense (SECDEF) strategic guidance provided to DoD in 2012 which noted among the primary missions of the U.S. armed forces was the ability to operate effectively in cyberspace and space. Specifically, the former SECDEF’s strategic guidance, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, stated that “Modern armed forces cannot conduct high-tempo, effective operations without reliable information and communication networks and assured access to cyberspace and space.”² For forward deployed U.S. naval forces and in consonance with his recent testimony to the House Armed Services Committee, Chief of

¹Department of Defense. 2014. *Quadrennial Defense Review Report: March 4, 2014*, Washington, D.C., p. 7.

²Department of Defense. 2012. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Washington, D.C., January.

Naval Operations (CNO) Admiral Jonathan W. Greenert noted the need to “sustain or enhance the Navy’s asymmetric capabilities in the physical domains as well in cyberspace and the electromagnetic spectrum.”³

In order to conduct operations successfully and defend its capabilities against all warfighting domains, many have warned DoD of the severity of the cyber threat and called for greater attention to defending against potential cyber attacks. For several years, many within and outside DoD have called for even greater attention to addressing threats to cyberspace. For example, a 2013 Defense Science Board (DSB) task force examined the resiliency of DoD systems to cyber attack and stated the following upfront in its report:

“The United States cannot be confident that our critical Information Technology (IT) systems will work under attack from a sophisticated and well-resourced opponent utilizing cyber capabilities in combination with all of their military and intelligence capabilities (a “full spectrum” adversary). While this is also true for others (e.g., Allies, rivals, and public/private networks), this Task Force strongly believes the DoD needs to take the lead and build an effective response to measurably increase confidence in the IT systems we depend on (public and private) and at the same time decrease a would-be attacker’s confidence in the effectiveness of their capabilities to compromise DoD systems. We have recommended an approach to do so, and we need to start now!”⁴

Outside of DoD and specifically in a report focused on U.S. naval forces, a 2010 National Research Council (NRC) report entitled *Information Assurance for Network-Centric Naval Forces*, conducted under the auspices of the Naval Studies Board (NSB), stated the following as one of its major findings:

“Cyber threats change on a timescale much shorter than the DoD acquisition life cycle for developing and deploying cyber security technologies. There are increasing

³Statement of Admiral Jonathan W. Greenert, USN, Chief of Naval Operations Before the House Armed Services Committee on FY 2015 Department of the Navy Posture, 12 March 2014.

⁴Defense Science Board Task Force. 2013. *Resilient Military Systems and the Advanced Cyber Threat*, Washington, D.C., January.

risks from these cyber threats, including risks of being unable to respond to assigned warfighting missions. Rapid acquisition and fielding of information assurance solutions are critical, but the committee did not see processes being put into place to support this need.”⁵

In an effort to better and more readily defend itself against cyber attacks, the former CNO established the position Commander, U.S. Fleet Cyber Command (COMFLTCYBERCOM), with responsibilities for serving as the Navy Component Commander to U.S. Cyber Command, in January 2010.⁶ A more recent organizational change, directed by the current CNO in March 2014, called for the establishment of an Information Dominance Type Command by October 2014 “to support Combatant Commanders and Navy Commanders ashore and afloat by providing forward deployable, sustainable, combat-ready Information Dominance forces.”⁷ While the committee views these organizational changes as positive steps, much work remains across the Navy in order to improve its cyber defense posture.

Along these lines, the current CNO requested that the NSB through the NRC conduct a study to review the U.S. Navy’s cyber defense capabilities.⁸ Subsequent to ensuring that all the necessary contracting and industrial security requirements were met, the NRC Chair appointed the Committee for a Review of U.S. Navy Cyber Defense Capabilities.

⁵National Research Council. 2010. *Information Assurance for Network-Centric Naval Forces*, The National Academies Press, Washington, D.C.

⁶In addition, with the former CNO’s recommissioning of U.S. Tenth Fleet (a former numbered fleet that was established in World War II to address the challenges presented by enemy submarine threats), COMFLTCYBERCOM also serves as Commander, U.S. Tenth Fleet (C10F). In total, COMFLTCYBERCOM/C10F has responsibilities for organizing and directing Navy cryptologic operations worldwide and integrating information operations and space planning as directed.

⁷Department of the Navy. March 11, 2014. “Establishing a Navy Information Dominance Type Command” by Joseph F. Gradisher. http://www.navy.mil/submit/display.asp?story_id=79601

⁸ADM Jonathan W. Greenert, USN, CNO, letter dated December 2011, to Dr. Ralph Cicerone, President, National Academy of Sciences.

In addition to reviewing cyber defense-related studies conducted within and outside the U.S. government, the specific terms of reference for the study (i.e., the committee's charge) were as follows:

- (1) Review U.S. Navy information technology modernization plans and processes with respect to the evolving threat and robustness to cyber attack, and identify any shortcomings;
- (2) Recommend any immediate operational and technical mitigation strategies needed to address any shortcomings identified above, as well as recommend any future mitigation strategies, including any architectural and procedural changes that would lead to more resilient naval systems and more robust network and communications capabilities given the evolving threat;
- (3) Review and assess the adequacy of current Department of the Navy policies, strategies, approaches, and investments in comparison to the findings and recommendations to both (1) and (2) above; and
- (4) Identify any other critical issue—not addressed in this study—that the U.S. Navy should consider addressing in subsequent studies.

APPROACH

The committee convened in October 2013 and held the following meetings over a course a 9-month period.

October 8-10, 2013, in Washington, D.C. First full committee meeting. Briefings on cyber defense perspectives from Deputy Assistant Chief of Staff for Intelligence, U.S. Fleet Cyber Command/U.S. TENTH Fleet; Assistant Chief of Staff for Plans and Policy, U.S. Fleet Cyber Command/U.S. TENTH Fleet; information dominance perspective from Director, Warfare Integration Directorate; and mission assurance considerations and cyber dependencies from Deputy Director, Warfare Integration for Information Dominance; U.S. Fleet Cyber

Command/U.S. TENTH Fleet; UHF SATCOM Requirements Office; and SPAWAR Systems Center-Atlantic.

November 19-21, 2013, in Washington, D.C. Second full committee meeting. Briefings on cyber considerations from Deputy Chief of Naval Operations for Fleet Readiness and Logistics; Chief Information Officer, Department of the Navy; Naval Facilities Engineering Command; Program Executive Officer for Littoral Combat Ship; Program Executive Officer for Integrated Warfare Systems; Deputy Chief of Naval Operations for Warfare Systems; Program Executive Officer for Enterprise Information Systems; Chief Engineer, Space and Naval Warfare Systems Command; Commander, U.S. Fleet Cyber Command/U.S. TENTH Fleet; and Assessment Division, Office of the Chief of Naval Operations.

December 16-17, 2013, in Washington, D.C. Third full committee meeting. Briefings on cyber considerations from Deputy Chief of Naval Operations for Information Dominance; Deputy Assistant Secretary of the Navy for Command, Communications, Intelligence, Information Operations and Space; Center for Strategic and International Studies; Program Executive Officer for Command, Control, Communications, Computers, and Intelligence; and Deputy Chief of Naval Operations for Operations, Plans, and Strategy.

January 21-23, 2014, in Washington, D.C. and Fort Meade, Maryland. Fourth full committee meeting. Briefings at National Security Agency on the Department of Defense Strategic Capability Office, Media Leaks Task Force, Threat Operations Center, Tailored Access Operation Operations/Offensive Cyber to Defensive Cyber Operations, Information Technology Architecture/Infrastructure perspectives, and cyber considerations of Marine Corps Forces Cyberspace Command. Briefings in Washington, D.C. on cyber considerations of Navy Strategic Systems Programs, Program Executive Officer for Submarines, Department of Defense Chief Information Officer, and Advanced Technology Panel.

February 18-20, 2014, in Washington, D.C. Fifth full committee meeting. Briefings on cyber defense activities at the Office of Naval Research, Naval Research Laboratory, Defense Advanced Research Projects Agency, MITRE Corporation, Sandia National Laboratories, Johns Hopkins University/Applied Physics Laboratory, Charles S. Draper Laboratory, Massachusetts Institute of Technology/Lincoln Laboratory, Intelligence Advanced Projects Research Agency, Amazon Web Services, Red Hat, McAfee Company, and National Science Foundation.

March 6-7, 2014, in San Diego, California. Site visit. Briefings from Space and Naval Warfare (SPAWAR) Systems Command on Computer Network Defense; Maritime Operations Center; Consolidated Afloat Network and Enterprise Services; Next Generation Enterprise Network; Joint Information Environment; Command and Control, and Intelligence, Surveillance, and Reconnaissance; Communications Systems and Program Executive Office Space Systems; Information Technology and Information Assurance Tech Authority; and SPAWAR Key Initiatives for Enhanced Cyber Security. Briefings from U.S. THIRD Fleet on Fleet Naval Forces Structure, Cyber Security Components, Identification of Cyber Dependencies of Operational Forces, Extensiveness of Cyber Degradations in Training and Exercises, Threats in Cyber Security Considerations, and Significant Challenges to Achieve an Adequate Cyber Security Posture.

March 25-27, 2014, in Washington, D.C. Sixth full committee meeting. Briefings on roles, responsibilities, authorities, and oversight of the Naval Nuclear Propulsion Program; Cyber and Its Potential Impact on Mission Assurance, Johns Hopkins University/Applied Physics

Laboratory; Cyber Defense Wargame, Office of the Deputy Chief of Naval Operations for Fleet Readiness and Logistics; Marine Corps Forces Cyberspace Command, Commanding General, MARFORCYBER; Strategic Systems Programs, Director for Strategic Systems Programs; Cyber Security, Intel Corporation; Office of Secretary of Defense for the Director of Operational Test and Evaluation; Naval Sea Systems Command; and Program Executive Officer for Tactical Air Programs.

April 17-18, 2014, in Suffolk, Virginia. Site visit. Briefings from Navy Cyber Defense Operations Command on cyber defense perspectives and activities at Navy Cyber Forces; Naval Network Warfare Command; Submarine Force, Atlantic; and Operational Test and Evaluation Force.

April 29-May 1, 2014, in Washington, D.C. Seventh full committee meeting. Briefings on roles, responsibilities, authorities, and oversight of Naval Sea Systems Command; U.S. Fleet Cyber Command/U.S. TENTH Fleet; and Navy Cyber Warfare Development Group.

After deliberating on and preparing its final report at its eighth and final meeting in June 2014, the committee submitted its final report for NRC external review in accordance with procedures approved by the NRC's Report Review Committee.

Acknowledgement of Reviewers

National Research Council reports are reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the NRC's Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published report as sound as possible and to ensure that the report meets institutional standards for objectivity, evidence, and responsiveness to the study charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of the draft (final) report:

William J. Fallon, USN (Ret.), CounterTack, Incorporated;
Anita K. Jones, University of Virginia;
John L. Manferdelli, University of California at Berkeley;
Roy A. Maxion, Carnegie Mellon University;

Jonathan M. Smith, University of Pennsylvania;
John P. Stenbit, Oakton, VA;
Steven J. Wallach, Convey Computer; and
Peter J. Weinberger, Google, Incorporated.

Although the reviewers listed above provided many constructive comments and suggestions, they were not asked to endorse the conclusions or recommendations, nor did they see the final report before release. The review of the draft report was overseen by William H. Press, University of Texas at Austin. Appointed by the NRC, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of the report rests entirely with the authoring committee and the institution.