

CENTER FOR CYBER WARFARE ESTABLISHED AT NPS

The newest research center at the Naval Postgraduate School is focused on the global cyber challenge. Established in the Department of Electrical and Computer Engineering, the Center for Cyber Warfare is a multi-departmental research center focusing on the general area of cyber warfare with emphasis on cyber attack. The research will support interdisciplinary graduate education for the cyber workforce. The fusion of faculty, staff and laboratories forming the center is illustrated below.

Cyberspace has been defined as “a global domain within the information environment, consisting of the interdependent network of information technology infra-

Cyber warfare must be an integral component of military operations. For example, anti-access or area denial requires multiple layers of offensive systems, utilizing the sea, land, air, space, and cyberspace. The purpose of a cyberspace strike is to deter the enemy, not to provoke combat. Thus, the objectives selected for a cyber strike must be few and precise. Important adversary information systems such as command and control centers, communications hubs, and other objectives might be targeted. This could impair the operation of adversaries’ systems and organizations and intimidate their policy makers.

The workforce that will staff the nation’s cyber organizations, both military and civilian, is currently skeletal and will need to grow in the years ahead. Some functions will require graduate education, and NPS is uniquely qualified to provide it. Research will also be required and should be an integral part of any graduate program.

The overarching strategy of the Center

for Cyber Warfare will be to bring focus to an effort to establish alliances between NPS, the operational forces, universities, and the intelligence community. Center research programs will support the education of a new generation of military officers and civilians who will constitute the cyber workforce.

Alliances will be forged through a program of outreach by the center’s business group. Center research will assure that related cyber-focused graduate courses remain on the leading edge. The center will bring together existing labs and create new labs to support faculty research and strive to establish a campus-wide secure laboratory environment for cyber research and education. NPS currently has a certified classified environment with adequate spaces, secure connectivity, and some existing funding for classified research and education. It is anticipated that top secret SCI billets will be obtained for faculty, staff, and students at NPS through ODNI sponsored agencies (NSA, NRO, CIA, NGA, and DIA). Through relationships with these agencies, a research program will be established that

supports cyber-centric graduate education for the Navy, DoD, and nation, ensuring a cyber workforce prepared to meet the challenges of the 21st century.

Mission

The mission of the Center for Cyber Warfare is to conduct sponsored cyberspace research in support of graduate education for the cyber workforce.

Vision

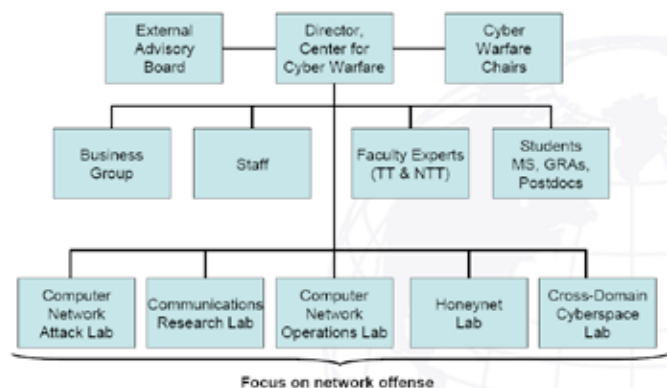
The vision of the Center for Cyber Warfare is to achieve national recognition of the NPS Cyber Program excellence, demand for program graduates, and a robust student enrollment in an interdisciplinary cyber curriculum.

Products and Services

The primary product of the center will be research results, both theoretical and applied, as they relate to problems associated with the cyber domain, computer-network operations, information operations, and signals intelligence. Such results typically take the form of techniques, models, simulations, computer programs, or theoretical analyses and are documented in student theses or dissertations, technical reports, conference presentations, and archival publications in the classified and unclassified literature.

Center Membership

- Professor Jeffrey B. Knorr, ECE, Interim Center Director
- Professor John McEachen, ECE
- Professor Murali Tummala, ECE
- Assistant Professor Weilan Su, ECE
- Professor Clark Robertson, ECE
- Professor Tri Ha, ECE
- Assistant Professor Frank Kragh, ECE
- Professor Bret Michael, CS and ECE
- Senior Lecturer Chris Eagle, CS
- Professor of Practice George Dinolt, CS
- Research Professor David Ford, PH



structures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” This describes a physical environment that will become a new domain for warfare along with subsurface, surface, land, air, and space, in which we must develop capabilities to detect, exploit, attack and protect signals and systems. To combat new, global, and increasingly complex national cyber security threats, the U.S. Navy, DoD and the nation must employ, educate, train, develop, and retain a dynamic, agile, technical, military and civilian cyber workforce that can utilize current information technology coupled with proficiency, perspective, experience, and expertise to counter threats in cyberspace.

NPS’ ability to meet this challenge depends on a well-educated, effective cyber workforce. Just as corporate America has recognized the value of cyber technology to gain and sustain competitive advantage, the government and DoD must gain and sustain competitive advantage in defending against adversaries, protecting citizens, and preserving national security.