SPAWAR
Systems Center
PACIFIC

CYBER

Cyberspace is a warfighting domain that is critical to ensuring the Navy's capability to operate forward. SSC Pacific's integrated cyber operations enable U.S. Navy warfighting capabilities in a contended cyberspace by delivering unique value to the warfighter in the cyber domain through end-to-end communications, computing, and software applications to dramatically improve warfighter mission outcomes.

SSC Pacific has a cyberspace/information technology workforce of more than 1100 personnel, more than 94 percent of whom maintain commercial certifications.

Our cyber efforts involve a close coupling of computer network defense, computer network exploitation, computer network development, and engineering. This enables U.S. forces to maneuver in the cyber domain while denying the adversary's ability to do the same and simultaneously protecting U.S. critical infrastructure and information.

SSC Pacific Unique Cyber Capabilities

- Full-spectrum cyberspace operations, defensive cyberspace operations (DCO), offensive Cyberspace Operations (OCO), Computer network exploitation (CNE), Department of Defense Information Network (DoDIN) operations
- Security engineering, certification & accreditation, risk management
- Cyber situational awareness, high assurance/ highly robust systems
- Information/network warfare
- Forensics

Today, U.S. Navy and other military services must take action to protect and operate within the cyber warfighting domain. SSC Pacific has a long history illustrating how the Navy has utilized technological advances across the cyber domain to maintain that critical warfighting advantage over all adversaries.

Some of SSC Pacific's current cyber efforts include:

- Navy's technical authority for cyber testing of acquisition programs
- Stochastic Compiler Hacks as Software Immunization Mechanisms (SCHSIM) develops artificial software diversity to minimize an attacker's knowledge of individual computer systems
- Cyber supervisory control and data acquisition

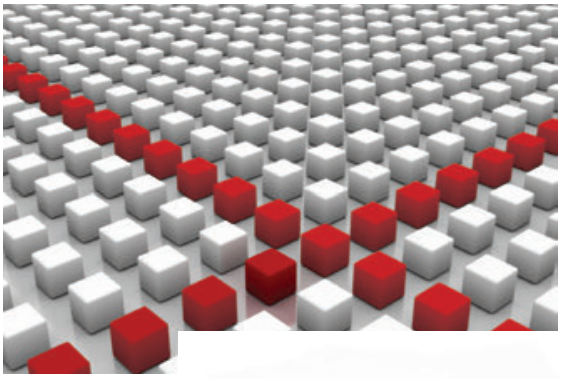
With the Warfighter

Protecting the warfighters' communication tools is of critical importance. SSC Pacific ensures interoperability of high-assurance devices by providing the National Security Agency (NSA) with systems engineering, standards development, interoperability, test engineering, and acquisition support. As the NSA-endorsed High Assurance Internet Protocol Encryptor (HAIPE) Interoperability Specification (IS) requirement conformance test facility, SSC Pacific certifies interoperability compliance of all HAIPE products.

Support from SSC Pacific personnel has allowed for the rapid advancement of high-assurance IP encryption by researching and reviewing innovative protocols and developing and implementing new technologies.

Explosive Ordnance Disposal Unmanned Underwater Vehicles (EOD UUV) project.

Stealthnet simulates an Army Brigade Combat Team soldier radio network that connects lower echelon soldiers to one another and back to their leaders. (Photo credit: Claire Heininger, U.S. Army).



Using the same software everywhere has made systems more vulnerable.

Inspired by bio-diversity, SCHISM is immunizing software systems against hacking.

Space and Naval Warfare Systems Center Pacific (SSC Pacific)
53560 Hull Street San Diego, California 92152-5001
Public Affairs Office: (619) 553-2717
www.spawar.navy.mil/pacific

SD 1521 • June 2016 JN16281
SSC Pacific, San Diego, CA 92152-5001