



CYBER OPERATIONS



Cyberspace is a critical warfighting domain that ensures the Navy's capability to operate forward. Space and Naval Warfare Systems Center Pacific's (NIWC Pacific) integrated cyber operations enable U.S. Navy warfighting capabilities in a contested cyberspace by delivering unique value to the warfighter through end-to-end communications, computing, and software applications to dramatically improve warfighter mission outcomes. NIWC 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 attack and 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.

NIWC Pacific's Unique Cyber Capabilities

- Holistic Cyber Science and Technology
- Cybersecurity Architectures and Engineering
- Cryptographic, Key Management and Cross Domain Solution (CDS) Engineering
- Computer Network Defense (CND) Engineering
- Cyber Risk to Mission Assessments/Assessment and Accreditation/Risk Management

- Penetration Testing/Forensic Analysis
- Information/Network Warfare
- Offensive Cyber Tool Development

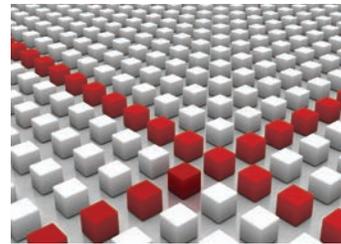
Today, U.S. Navy and other military services must take action to protect and operate within the cyber warfighting domain. NIWC Pacific has a long history assisting the Navy in utilizing technological advances across the cyber domain to maintain that critical warfighting advantage over all adversaries.

Some of NIWC Pacific's current cyber efforts

- **Navy Cyber Situational Awareness (NCSA):** Developing capability for NCSA to collate data, analytics, visualizations, interfaces, and infrastructure for the Navy's cyber terrain.
- **Vulnerability Remediation Asset Manager (VRAM):** Developing/sustaining VRAM, a web-enabled asset management, network vulnerability data repository and monitoring tool providing cyber directive compliance reporting capabilities
- **SHARKCAGE:** Developing a capability for a global Navy Defense Cyber Operations (DCO) enclave that enables: (1) visibility from external Navy boundary to tactical edge, to include Platform IT (PIT) systems and networks, and (2) monitoring and decision support within decision cycle of adversary rapid technology engineering and insertion

- **IA/Cybersecurity Technical Authority:** Supporting the Navy Information Assurance Technical Authority (IA TA) to establish, monitor, and approve technical standards, tools, and processes that promote Navy information dominance by identifying and mitigating cybersecurity risks and improving the cybersecurity posture of the Navy
- **Key Management Engineering:** Navy lead engineer for key management infrastructure (KMI), supporting KMI/electronic key management system (EKMS) integration. Developing/sustaining a next-generation key management system, iApp, transforming operations to a more secure automated distribution of keys
- **Cybersecurity Engineering:** Employing information systems security engineering to conceive, design, develop, verify, and validate information assurance insertion into Department of Defense (DoD) and federal information
- **Cybersecurity Risk Management:** Performing risk assessments and mitigations across the lifecycle of developed systems
- **Crypto Modernization Engineering:** Engineering and software development agent to: develop interoperability test requirements and tools for high assurance internet protocol encryptor (HAiPE), Tactical Secure Voice (TSV) Link Encryptor Family (LEF), and transmission security (TRANSEC) products; evaluate cryptographic devices, support enterprise acquisition of interoperable cryptographic solutions
- **Computer Network Defense (CND) Engineering:** Providing scalable CND security solutions for the fleet to protect against cyber threats through real time protection, detection and reaction. Integrating information assurance tools into engineering solutions in accordance with Chief Technology Officer mandates
- **PKI/Identity Management:** Providing research, development, test and evaluation (RDT&E) and sustainment support to naval assets using cryptographic logon (CLO), online certificate status protocol (OCSP), and identity management
- **Cyber Mission Forces (CMF) Toolkits:** Developing Navy Cyber Protection Team (CPT) toolkits and deployable mission support system Navy toolkits
- **Offensive Cyber Tool Development (OCTDEV):** Supporting capability to rapidly develop cyber tools for use by the Navy and Marine Corps in the tactical maritime and expeditionary environment

- **Cyber Autonomic Network Distributed Immune Response (CANDIR):** Developing/sustaining an extensible, closed loop, autonomic computing system that provides active defense and offensive countermeasures to systems/networks anomalies, malware, and changes to threat conditions
- **Cybersecurity Science & Technology (S&T):** Conducting full-spectrum cyber S&T from basic research in cryptographic algorithm development to applied research in mobile applications and environments to more advanced research in critical infrastructures and embedded systems cybersecurity
- **Cyber Testing:** Developing tools and techniques to conduct cybersecurity assessments and operational testing to include penetration testing and vulnerability scanning
- **Software Assurance:** Providing software security engineering and software security testing support to NIWC Pacific, program executive officer/command, control, communications, and intelligence (PEO C4I) and Navy programs. Developing tools, practices, and processes to conduct SwA activities in support of Navy programs/projects and business applications
- **Stochastic Compiler Hacks as Software Immunization Mechanisms (SCHISM):** Develops artificial software diversity to minimize an attacker's knowledge of individual computer systems.



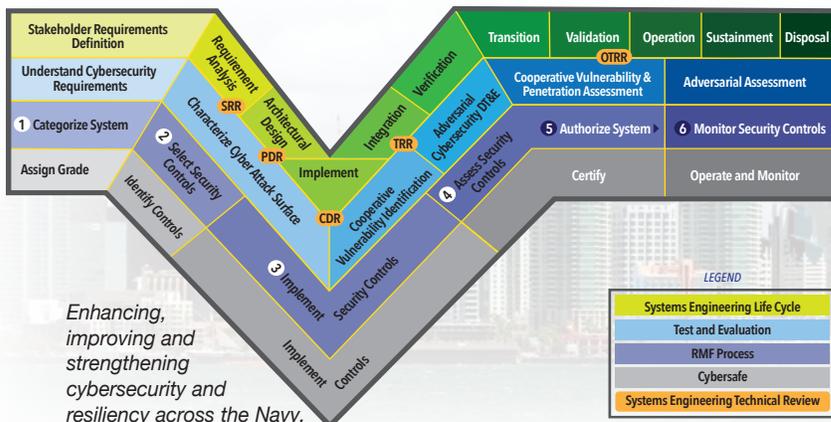
Using the same software everywhere has made systems more vulnerable.



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

With the Warfighter

The Integrated Cyber Operations (ICO) portfolio provides mission assurance to all critical missions of the Navy ranging from strategic nuclear command and control and communications (NC3) and ballistic missile defense (BMD) to tactical air defense and strike warfare. The portfolio also develops and provides tools to fleet commanders for defensive operations and offensive computer network operations.



We provide mission assurance and resilience which is the ability to resist, absorb, and recover from adverse actions that may cause harm, destruction or loss of ability to perform mission-related functions. Our defensive cybersecurity systems protect and defend against malicious attacks and detect adversarial actions to penetrate and exploit our mission-critical systems. Likewise, our offensive cyber capabilities provide operational commanders the ability to exploit and deny adversarial abilities to use cyberspace.

For more information

Naval Information Warfare Center Pacific (NIWC Pacific)
 53560 Hull Street, San Diego, California 92152-5001
 Public Affairs Office: (619) 553-2717
www.public.navy.mil/navwar/NIWC-Pacific