Cyberspace Defense in Denied, Degraded and Disconnected Environments (Cyber) Advanced Naval Technology Exercise (ANTX)

6-16 September 2022
Charleston, SC

Naval Information Warfare Center ATLANTIC

Naval Information Warfare Center PACIFIC

Table of Contents

	PAGE
About Cyber ANTX	3
NIWC Atlantic at a Glance	4
NCRC	5
Technologies/Focus Areas	6/7
Notes	8

About Cyber ANTX

The Department of the Navy (DON) Cyberspace Defense in Denied, Degraded and Disconnected Environments (Cyber) Advanced Naval Technology Exercise (ANTX) is the first exercise conducted at Naval Information Warfare Center (NIWC) Atlantic on the National Cyber Range Complex (NCRC). NIWC Atlantic and NCRC executed and sponsored the Cyber ANTX along with U.S. Fleet Cyber Command/U.S. TENTH Fleet (FCC/C10F), Naval Information Warfighting Development Center (NIWDC), NIWC Pacific, Naval Information Warfare Systems Command (NAVWAR) Program Executive Office (PEO) C4I PMW 130, and Marine Corps Forces Cyberspace Command (MARFORCYBER) G9. The DON sought technologies for the Cyber ANTX that enable ashore support to cyber defenders who are afloat or in other environments and who may be experiencing denied, degraded or oftentimes disconnected communications. These local cyber defenders have an especially challenging job on afloat platforms. A current challenge within the DON is retaining highly specialized expertise on most ships. The important military value of these platforms further aggravates the problem, since combat-critical systems are a known target for advanced persistent threats.

The Cyber ANTX evaluates technologies that:

- Allow a highly skilled ashore team to “quarterback” cyber incident response on several ships at once;
- Better inform and empower Local Defenders before, during and after a cyber incident;
- Summarize and simplify Indicator of Compromise (IOC) reporting;
- Efficiently emit cyber threat intelligence over Disrupted, Degraded, Intermittent, Latent (D-DIL) links;
- Allow ashore defenders to describe and recommend courses of action in a reliable, timely fashion;
- Empower Local Defenders to automate responses efficiently;
- Support efficient system restoration to “known good” states; and
- Anticipate and “pre-place” capabilities—with a sufficiently low learning curve—for local defender execution.

The Cyber ANTX used a Commercial Solutions Opening (CSO) to accept 29 proposals from industry, government and academia. The CSO provides opportunities for follow-on contracting, development and experimentation actions based on operational and technical assessments. The CSO may be leveraged by any organization in the Department of Defense (DoD) to support future procurement activities, with NAVWAR PEO C4I PMW 130 and FCC/C10F identified as the primary transition targets for the Cyber ANTX.

Naval Information Warfare Center ATLANTIC

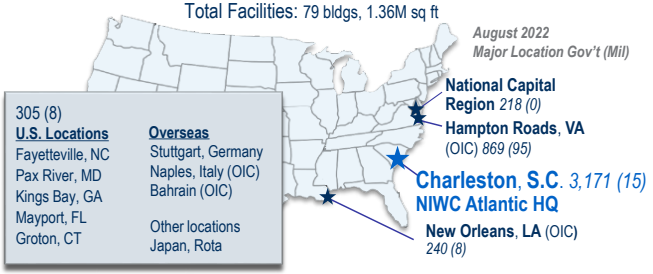
NIWC Atlantic at a Glance

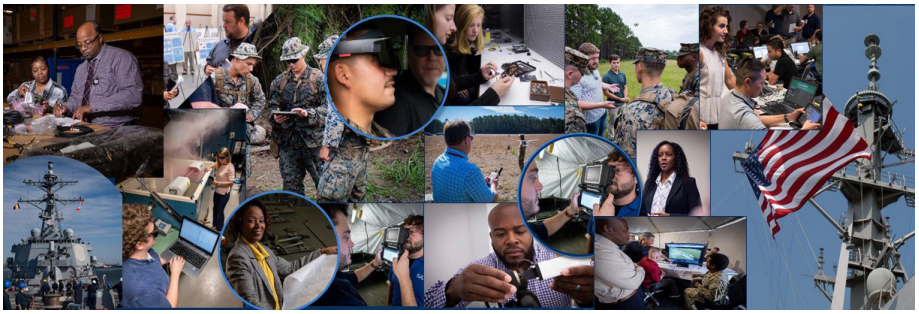
DELIVERING MISSION-CRITICAL INFORMATION WARFARE SOLUTIONS TO THE WARFIGHTER

Naval Information Warfare Center (NIWC) Atlantic is a Navy engineering and Information Technology (IT) command and part of the Naval Research and Development Establishment (NR&DE). Our work is shaped by requirements that demand research and engineering with the goal of delivering the operational advantage gained from fully integrating naval information functions, capabilities and resources to optimize decision making and maximize warfighting effects.

Major U.S. Locations

Total Facilities: 79 bldgs, 1.36M sq ft





MISSION:

Serve our nation by delivering information warfare solutions that protect national security.

VISION:

WIN THE INFORMATION WAR

NCRC NATIONAL CYBER RANGE COMPLEX CHARLESTON

The National Cyber Range Complex (NCRC) addresses our nation's most critical cybersecurity test and evaluation (T&E) and training challenges. The NCRC is operated by the Test Resource Management Center (TRMC) and authorized to operate by the Intelligence Community (IC), and provides expertise and enterprise infrastructure to plan and execute realistic cybersecurity tests, evaluations, experiments, mission rehearsal exercises and training events. The NCRC comprises multiple cyber ranges and a secure, distributed network infrastructure that not only connects the cyber ranges but allows for the integration of remote personnel, capabilities and facilities as well. NCRC Charleston and NCRC Patuxent River are the two Cyber Range complexes aligned with the Navy. N94 is the Navy's OPNAV sponsor. The cyber ranges provide representations of high-fidelity Department of Defense (DoD) systems, tactical environments, the commercial Internet, and of other "Red, Blue and Gray" commercial, administrative, tactical, government, and enterprise environments. These representations range from small, focused environments with a few systems to large- scale environments with thousands of systems. These environments are often augmented by human-in-the-loop (e.g., operators, opposing force, etc.) and hardware-in-the-loop (e.g., physical network components, tactical systems, etc.), along with customized traffic generation and instrumentation to create a more robust environment for event execution. The NCRC also provides users with a secure, controlled sandbox in which to conduct activities that would otherwise potentially be harmful or disruptive to production or operational environments.

Emulation of complex, operationally representative networked environments: Representative environments are designed to meet a user's specific requirements and objectives. The representations can include all layers of the Open Systems Interconnection (OSI) model: physical, data link, network, transport, session, presentation and applications.

Integrated Automation Framework provides significant efficiencies: Manual environment deployment may take several weeks or months, but automation enables the NCRC to deploy baseline environments in a few hours or days and allows NCRC to execute more events. Automation also minimizes the potential for human error and enables NCRC to replicate scenarios and phenomena.

Sanitization restores all exposed systems to a known clean state: Sanitization allows NCRC to reuse assets even when they are exposed to malicious and sophisticated uncharacterized code. In conjunction with NCRC's accredited security architecture and procedures, sanitization gives users unconstrained environments in which even sophisticated threats can be released with impunity.

Concurrently support multiple events at varying classifications: NCRC's accredited security architecture uses isolation capabilities to segregate events, users and data. This allows for maximized use of NCRC resources in support of user requirements.

Technical Support Team: The NCRC's multidisciplinary team works hand-in-hand with representatives from the DOD, intelligence community (IC), other government organizations, industry, and academia to successfully plan and execute events. NCRC's subject matter expertise includes offensive and defensive cybersecurity, IT services, test and evaluation, systems engineering, and malware development.

Typical use cases:

- Vulnerability assessments determine the resiliency of a system or system-of-system-of-systems including external dependencies and impact on mission effectiveness.
- Cyber Mission Force training provides realistic mission tailored unconstrained spaces to support training; certification; tactics, technique, and procedures (TTP) development; mission rehearsal; and exercises.
- Product/solution evaluations examine an increase or decrease in security posture when adding new components.
- Architecture evaluations remove lab constraints and evaluate system architectures at scale.
- Expanding capabilities include standardized bus architectures and industrial control systems.

Benefits:

- A highly scalable, secure, and extremely flexible range capability able to influence decision related considerations quickly, accurately and safely.
- Detailed empirical data analysis provides users with actionable information to support critical decision making during all phases of the acquisition life cycle.
- Instrumented sensors collect system data for reporting and after action review purposes.
- An expert cyber event engineering team provide planning, design, execution support, and post-execution reporting.
- "High fidelity" environments enable Cyber Mission Forces to train as they fight and offer testers an opportunity to assess vulnerabilities and mission impacts.

Technologies

FOCUS AREA

Containment & Prevention

TECHNOLOGY NAME	COMPANY
AttackIQ Security Optimization Platform	Insight Public Sector
Non-Destructive Inspection	Risk Mitigation Consulting, Inc.
Zero Trust	Illumio, Inc.
ZKX	REDCOM Laboratories, Inc.
TPCP	NIWC PAC/ONR
Defensive Cyber Catalog	NIWC PAC/ONR
Software Defined Perimeter (SDP)	Appgate Federal

Indications and Warnings

TECHNOLOGY NAME	COMPANY
CADO	Punch Cyber Corp.
CLAW	The Bellwether Group
PRIME POLARIS	Ardalyst

Monitoring and Analytics

TECHNOLOGY NAME	COMPANY
Combat Cloud Environment	ManTech
OPTIEx	Tychon, LLC
Predictive Attack Surface Detection	Tychon, LLC
BDP/LTAC	Enlighten IT Consulting, LLC
Cyber Precog Flyaway Kit	Booz Allen Hamilton
SOAR	SRC

Cloud Enabled Defense

TECHNOLOGY NAME	COMPANY
SOTF	Accenture Federal Services, LLC
IronNet	Booz Allen Hamilton
ENVE	BlackHorse

Technologies

FOCUS AREA

Malicious/Unauthorized Hardware Detection

TECHNOLOGY NAME	COMPANY
IdentiPHY	Applied Engineering Concepts, Inc.
DCX	Vision4CE LLC
CKUR	Vision4CE LLC
YOLO	Chip Scan

Malicious/Unauthorized Software Detection

TECHNOLOGY NAME	COMPANY
HOPAMA	Mayachitra, Inc.
Unified Cyber Platform (UPC)	World Wide Technology
HARPOON	World Wide Technology

Notes

Cyberspace Defense in Denied, Degraded and Disconnected Environments ANTX