Computer Network Defense Roadmap

Department of the Navy | Chief Information Officer

1.1

Foreword

Today, we operate in a net-centric environment, with the goal of information superiority. Achieving and sustaining this goal is heavily dependent on establishing, maintaining, and defending a secure and interoperable infrastructure – the "network." We must defend the network and protect the information. The threat to our infrastructure and information is advanced, persistent, sophisticated, always changing, and well resourced. Our challenge is to be more advanced, persistent, sophisticated, and ahead of the threat. We can do so by focusing smartly and effectively our increasingly limited resources, working with Government and industry to develop capabilities that allow us to be proactive, preemptive, and when necessary, reactive in real time. This roadmap will guide the Department of the Navy as we work with other defense components and agencies to make our investment decisions.

We must invest in capability that allows us to act proactively, but first we must measure accurately and consistently our detection and prevention of unwanted activity and behavior on our networks. This roadmap lays out the way ahead for computer network defense in the Department of the Navy.

John J. Lussier
Department of the Navy
Principal Deputy Chief Information Officer
Information Assurance Officer

Senior

Roadmap Purpose

The Department of the Navy (DON) Naval Networking Environment (NNE) ~2016 Strategic Definition, Scope and Strategy of May 2008, laid out a roadmap for guiding the DON toward a future net-centric environment. The roadmap presents a transition from today's environment composed of four enterprise computing and communications environments within the DON to NNE. The Naval Networking Environment will provide a highly secure and reliable enterprise-wide voice, video, and data network environment that focuses on the warfighter first, providing ubiquitous access to data, services, and applications from anywhere in the world.

Reliance on the DON information infrastructure continues to grow and the threats posed by adversaries are advanced, persistent, and always changing. The DON Information Assurance Policy provides the aligned defense-in-depth program for the DON. The purpose of the DON Computer Network Defense (CND) Roadmap is to communicate the DON strategy for sustaining and improving CND now and in the future as the DON transitions to NNE. In this age of network-centric warfare, computer and network technologies are diffused into virtually all military systems, and interconnected military units operate cohesively. CND is essential to achieving assured networked forces, information sharing, situational awareness, speed of command, and mission effectiveness.

The DON CND Roadmap demonstrates the ongoing nature of implementing CND to meet the range of computer network threats. It highlights the need for the Department to make informed decisions as we invest in our CND to optimize our network security posture. CND is not an episodic process; though it changes to meet the changing conditions posed by emerging threats and other real-world events. Additionally, the roadmap shows the high-level linkage of CND strategy to operations, the alignment of CND to the naval mission, and the importance of CND as it flows from the most senior levels of leadership within the DON. Finally, it shows that CND is everyone's job and makes clear the strategic outcomes of DON CND.

Roadmap Overview

The roadmap begins with an understanding of CND, and then continues on the logical continuum from mission to action to strategic outcomes. This continuum reveals the shared purpose of CND among all levels of the DON, and it links the flow and integration of resources and business processes to achieve the strategic outcomes. In other words, the CND Roadmap is about vertical alignment of CND from mission to outcome; see Figure 1.

Figure 1: Mission to Outcome CND Vertical Alignment

Computer Network Defense

Computer Network Defense is one of many elements of the more expansive and broadly defined cyberspace domain[1] (illustrated in Figure 2) and cyberspace operations[2]. The practice and discipline of CND is one of the three enablers of Computer Network Operations (CNO) and essential to all warfare domains. The three enablers of CNO are Computer Network Attack (CNA), Computer Network Exploitation (CNE), and CND.

CNA includes actions cyber warriors take using computer networks to disrupt, deny, degrade, or destroy an adversary's information resident in computers and computer networks, or the computers and networks themselves. CNE includes cyber activities enabling operations and intelligence collection capabilities, conducted using computer networks to gather data from target or adversary automated information systems or networks. CND includes actions cyber warriors take using computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within Department of Defense information systems and computer networks.

Information Assurance (IA) is much broader and includes measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. IA and all aspects of CNO are interrelated and rely upon each other to be effective.

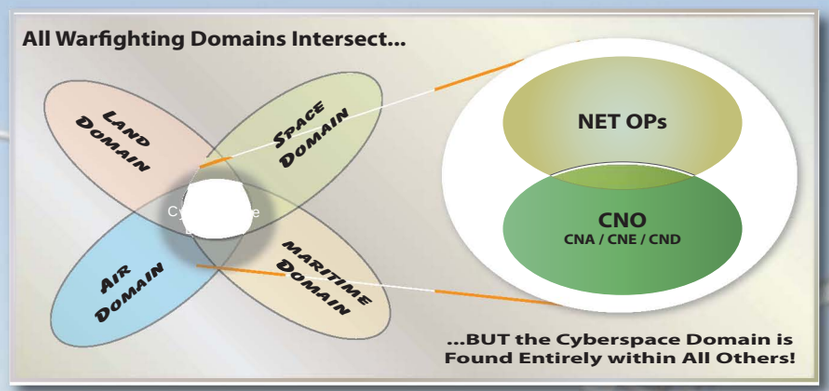


Figure 2: Cyberspace Domain

1 Cyberspace is a global domain within the information environment, consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (Deputy Secretary of Defense Memorandum dated 2 May 2008)

2 The term, cyberspace operations, has been proposed to mean the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid. (VCJS Memo to DEPSECDEF, Subject: Definition of Cyberspace Operations, dated 29 Sept 08)

Mission

The DON mission is to deliver a naval warfighting team – Navy and Marine Corps forces, trained, and equipped – to support the full range of missions that might serve as an instrument of national power and influence. This includes arming naval forces with secure and trusted systems and information, enabling them to fight and win. Therefore, the Navy and Marine Corps must deter, analyze, protect, monitor, and detect network activity in response to unauthorized activity within its computer and network systems. Additionally, the Navy and Marine Corps must coordinate with, and report unauthorized activities to, other CND service providers to ensure broader defense of the Global Information Grid (GIG).

Vision

The DON's vision is a naval warfighting team armed with the secure, appropriate, assured, accurate, and timely information to fight and win. In the cyber age, this means naval forces able to continue operations across the spectrum of conflict. For CND this means integrated capabilities and technologies where policy, compliance, configuration management, patch and vulnerability management, and threat detection and response are coordinated and synergistic, delivering maximum benefit to defending the network.

Strategy

Goal 2 of the DON Information Management (IM) and Information Technology (IT) Strategic Plan states:

"Protect and defend our naval critical infrastructures, networks, and information to maximize mission assurance."

To date, the DON CND strategy, like the DON IA strategy, is one of defense-in-depth to protect DON information and information systems. This strategy must ensure continued operation of naval networks to support and conduct the mission, even if in a degraded state. All of this is performed in a complex and constantly changing environment. Defense-in-depth is a layered approach, which forces adversaries to penetrate multiple protection layers, decreasing the likelihood of their success. It is founded on the principle of a strong IA posture and relies on an effective triad of people, technology, and CND operations.

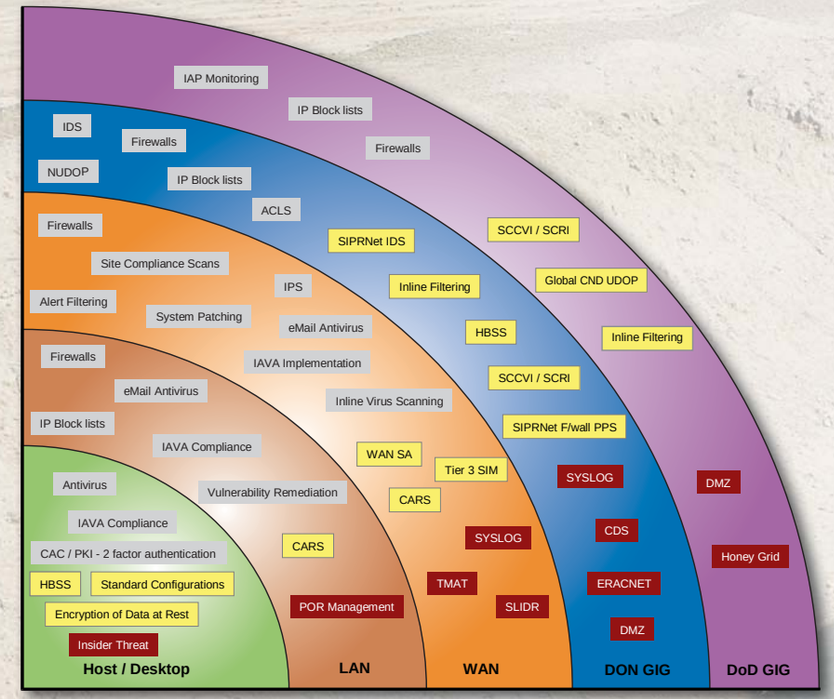


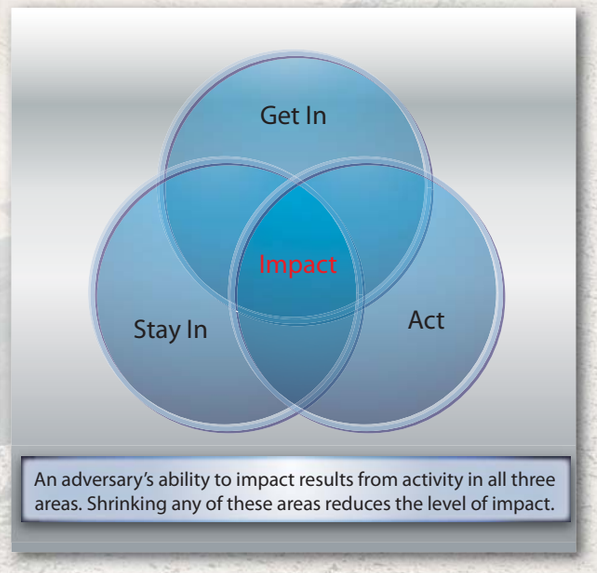
Figure 3: Computer Network Defense
Defense-in-Depth

Strategic Outcomes

The strategic outcome of the DON CND strategy is information and a network infrastructure we can trust. In other words, the result of the strategy is to minimize the impact of adversaries' actions. Using the Johns Hopkins University Applied Physics Laboratory's National Information Assurance Engagement Center model, illustrated in Figure 4, we must protect against an adversary's ability to get in, stay in, and act. From the DON perspective, we must protect against an adversary's ability to get in naval networks, stay in naval networks, and act on naval information and networks.

This model illustrates the need to protect and react with a strategy in which the DON proportions defense-in-depth across all three spheres, thereby reducing the adversary's impact on naval network infrastructure and information.

The DON CND strategy targets an adversary's ability to get in, stay in, and act within the cyberspace domain. Naval network operators and defenders will implement the CND strategy in a complex and constantly changing environment. The DON CND is a new approach to defense-in-depth; however, it is still a layered approach, which



f o r c e s
dversaries
o penetrate or try
o operate through
ultiple protection
ayers, decreasing
he likelihood of
uccess. Founded
n the principle of
strong IA posture,
ON CND relies
n an effective
riad of people,
echnology, and
ND operations.

CND Service Providers

The DoD requires all owners of information systems and networks to have CND capability. Within the DON, the Navy and Marine Corps established CND service through the Navy Cyber Defense Operations Command (NCDOC) and the Marine Corps Network Operations and Security Center (MCNOSC), respectively. The DON elements of CND are under the operational coordination and direction of a single lead, the United States Strategic Command, Joint Task Force-Global Network Operations (JTF-GNO), to conduct multi-component and defense-wide CND operations on the GIG.

The primary CND service areas are protect; monitor; analyze and detect; and respond. These services include actions used for preventing or mitigating computer network attacks that may cause disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems, or the theft of information.

CND Initiatives

The unique requirements of the DoD and DON drive CND initiatives. Within the DON, there are many efforts and activities underway to evolve and continually improve CND posture and capabilities. The following are some of the major initiatives underway:

- **Prometheus.** To aggregate, correlate, fuse, analyze, display, and disseminate disparate data from a wide variety of sources to produce the Network Domain Awareness required to aggressively defend Navy enterprise networks, the DON has implemented and continued to expand the capabilities of the Prometheus system.

- **Secure Configuration Compliance Validation Initiative (SCCVI) and Secure Configuration Remediation Initiative (SCRI).** To check for secure configurations, and automate the remediation process, ensuring that non-compliant systems return to a secure configuration, the DON is implementing SCCVI and SCRI.

  - » **SCCVI is a tool to discover vulnerabilities and check compliance with Information Assurance Vulnerability Alerts (IAVA).** It is a discovery and audit capability; it discovers assets and identifies known security vulnerabilities on a number of different platforms and technologies, including servers, databases, switches, routers, and wireless access points.

  - » **SCRI is a tool to push IAVA patches to non-compliant systems, bringing them into compliance with policies; it implements corrective actions to eliminate or mitigate identified vulnerability.**

- **Host Based Security System (HBSS).** To detect and counter, in real-time, against known cyber-threats, the DON is implementing HBSS. The HBSS protects host machines from exploits and malicious activity, providing a centrally managed Host Based Firewall System and Host Based Intrusion Prevention System, which delivers robust buffer overflow protection, signature and behavioral based intrusion protection, and application monitoring.

- **Adware and Spyware Detection, Eradication and Protection (SDEP).** For Adware and SDEP the DON is relying on capability offered through the HBSS initiative.

- **User Defined Operational Picture (UDOP).** To enable individuals or communities of interest to develop and understand activity and behavior on their systems and networks, the DON is developing and implementing a capability to share a common understanding, improve situational awareness,

and improve command and control of the networks. The DON is achieving this through the UDOP effort that delivers a portal with tailored content to meet the needs of individuals and communities of interest.

- **DoD Insider Threat Detection Initiative.** To address the Insider Threat, the DON is participating in the DoD Insider Threat Detection initiative, which developed and is deploying an Insider Threat Focused Observation Tool (InTFOT).

- **NIPRNET DMZ.** To add protection between internal and external networks, the DON, working with the National Security Agency (NSA) and Defense Information Systems Agency (DISA), developed a new demilitarized zone (DMZ) architecture for the NIPRNET. The DON is implementing the new DMZ architecture as it strengthens internal network IA policy for external information exchange. A DMZ provides external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

- **Intrusion Protection Systems (IPS).** To monitor networks and system activities for malicious or unwanted behavior, and to allow network defenders to take decisive action in real-time, to block or prevent such activities, the DON is implementing IPS.

- **Intelligent Agent Security Manager (IASM).** To perform near real-time acquisition and normalization of security event logs and alerts from network and host sensors, firewalls, routers, and operating systems; and to perform signature-based analyses of normalized events, allowing anomaly-based assessment of events, which generates alarms about unique security attacks, the DON is implementing IASM. The IASM watches network traffic on many levels to determine misuse, fraud, or attack. It collects, normalizes, correlates, and analyzes data to determine cyber attack profiles in real time.

- **Data at Rest (DAR) Encryption.** To protect sensitive, unclassified data residing on government laptops, other mobile computing devices, and removable storage media devices, the DON is implementing a DAR encryption solution.

- **User CND Awareness.** To ensure computer and network users are fully aware of the threat and their responsibilities in thwarting that threat, the DON is continuing to emphasize, and is increasing, user awareness.

- **Cryptographic Log On (CLO).** To improve the security of DON networks, the reliance on usernames and passwords is being eliminated, and DON networks are transitioning fully to cryptographic logon.

- **Hardware Token Use.** To reduce the inherent vulnerabilities of soft PKI certificates, the DON is fully committed to transitioning to hardware tokens (i.e., Common Access Cards, alternate tokens, hardware-based external certificate authority tokens, and federated hardware-based PKI tokens).

- **Federal Desktop Core Configuration (FDCC).** To provide a single standard enterprise-wide managed environment for desktops and laptops running a Microsoft Windows operating system, and by using a common configuration developed for the enterprise rather than hundreds of costly locally created configurations, the DON will improve security, reduce costs, and reduce application compatibility issues. The chief way of successfully attaining compliance with the FDCC is through the Security Content Automation Protocol (SCAP), which uses specific standards that automate the way computers detect vulnerabilities and verify that computers are following required security policies.

- **Web Content Filtering.** To provide real-time protection against malware, spyware, malicious mobile code, and other inappropriate content from entering the network, the DON is deploying a Web content filtering capability.

- **CND Afloat.** For ships, the Navy is implementing Afloat CND Suites consisting of SCCVI, SCRI, and HBSS. On selected large deck platforms, IPS is being installed.

The Map Ahead

The threat is advanced, persistent, and constantly changing, making it an imperative that DON CND be more advanced, persistent, and as flexible and adaptable as possible to the changing threat. This means having the right data and information, and understanding the activity and behavior of the users and the DON systems and networks they use, in order to detect inappropriate activity and behavior and take proper action in real-time.

To ensure the Department meets the challenge of the future threat, the DON will continue with comprehensive, layered defense – the Defense-in-Depth Strategy. DON CND will move forward, aggressively protecting against known threats and proactively addressing emerging and unknown threats. Emerging and unknown threats are the most difficult and challenging to address. However, mitigation is possible by moving DON CND from a collection of point solutions that do not give us the comprehensive visibility of users and activity on DON systems and networks, to solutions that enable us to know and understand acceptable use and behavior of users, systems, and networks. This requires collecting, correlating, and analyzing data in real time. DON CND will accomplish this by moving to a more rational, well-integrated suite of capabilities, enabled by current, emerging, and future technologies.

In addition to a changing threat, the increasing popularity of collaborative Web applications such as blogs, social networks, podcasts, and wikis, and mobile end-user devices, has brought a new set of challenges to CND.

The DON will work with the JTF-GNO and other organizations through the governance processes to determine specific products and tools to achieve and sustain the level of CND vital to mission success. Synergy will be created through people, processes, and technology. The future of DON CND will include the following, which are presented in order of consideration for investment, given our current CND capabilities.

- **Advanced Network Access Control (NAC).** This capability allows evaluation of the security state of devices connecting to the network. Once connected to the network, it continuously monitors these devices and applies necessary remediation policies based on the state of the device. It enables managing all end-points of the network, including those devices connecting from outside the network's first perimeter of defense – the firewall – providing true point protection at the edge. The DON will integrate NAC fully within an overarching, full spectrum enterprise access control schema that supports the end-to-end requirements in a coalition, first responder/non-government organization (NGO) environment that accounts for differences in trust levels of these various environments.

- **Enhanced – Next Generation – IPS.** This technology improves detection and remediation capabilities, working real-time and proactively, and looking at different layers in the protocol stack. It delivers a more comprehensive content inspection, using sophisticated detection techniques that extend beyond simple keyword matching; and, unlike anomaly detection solutions, which require time to learn and baseline normal traffic, the pattern and behavioral profiles work immediately to provide instant value with minimal false positives.

- **Enhanced Anti-Malware Technology.** This technology goes beyond signature-based detection and remediation. It supports real-time and in-line detection and remediation and delivers comprehensive scanning to discover and eliminate Rootkits and other deeply planted elements of mal-activity. Additionally, this enhanced capability will protect against zero-day threats, which are threats for which a signature or remedy is not known or available. This technology will support behavioral-based protection.

- **Reduced Administration / Management Complexity.** Through automation, we will reduce complexity of network and system administration and management. We will acquire capability that delivers a more complete picture of activity of users, systems, and networks. This capability will rely upon audit and event logs, correlate the data, and alert network operators and defenders to suspicious behavior. Naval network operators and defenders will deal with the complexity and sophistication of network and system administration and management through a console interface behind which automated activities are collecting, correlating, and analyzing network and system data, and reporting user and network activity and behavior to the operator and defender. Additionally, naval network operators and defenders will be able to set and enable proactive features such as automatic, real-time response and notification to threats. Additionally, we will integrate this secure management capability into the overall network management capability.

- **Recognize Virtual Environments.** CND capabilities must be able to recognize virtual environments and protect virtual images, both active-online and inactive-offline, by enforcing security policies across all virtual machines and archived images as they are made active.

- **Advanced Forensics Capability.** This capability introduces correlation of post-incident/attack forensics with pre-incident/attack forensics, and delivers persistent state monitoring. This capability supports learning and understanding of user, system, and network behavior and facilitates understanding the norm, thereby enabling proactive response to abnormal activity and behavior on systems and networks.

Department of the Navy
Chief Information Officer

1000 Navy Pentagon
Washington, DC 20350-1000
www.doncio.navy.mil

Version 1.1 May 2009

Photo Credits

Cover: Cpl. Christopher R. Rye (041222-M-6237R-009), Pg 2-3 Mass Communication Specialist 1st Class Denny Cantrell (090215-N-8517C-676), Pg 4-5 Mass Communication Specialist 2nd Class Gary A. Prill (090319-N-7730P-161), Pg 6-7 Lance Cpl. Ronald W. Stauffer (090105-M-9999S-077), Pg 8-9 Mass Communication Specialist 3rd Class Justin M. Smelley (090502-N-2858S-126), Pg 10-11 Lance Cpl. Monty Burton (090110-M-8478B-011), Pg 12-13 Cpl Mike Escobar (050719-M-0502E-010), Pg 14-15 Mass Communication Specialist 2nd Class Greg Johnson (090215-N-9950J-101), Pg 16-17 Cpl. Pete Thibodeau (090124-M-6159T-052), Pg 18-19 Mass Communication Specialist 2nd Class Jesse B. Awalt (090401-N-0506A-630)