

# NMCI Active Computer Network Defense Strategy: Cyber-Centric Maneuver Warfare

## 1. Introduction

*Leaning into the 21st Century - The Changing Face of Warfare*

“They will attack us asymmetrically, pitting their strength against our weakness, whether that lies in the military, political, or domestic realm. For example, in future conflicts, data lines of communication may be just as important as sea lines of communication -- and our adversaries, whether they are third world nations, transnational actors, or crime syndicates, will attack them.”

*General Krulak, Former Commandant of the Marine Corps*

*Navy Information Warfare Strategic Plan: IW – Capabilities for the New Millennium*

“Joint Vision 2010 provides us a vision of future warfare in which US forces will enjoy full spectrum dominance by achieving total Information Superiority. The basis for this framework lies in command and control and intelligence, along with other applications of new technology, which will transform the traditional military functions of maneuver, strike, protection and logistics. ... Achieving the level of information superiority needed to facilitate this revolution in military operations requires the services to develop both Offensive and Defensive IW capabilities.”

*Admiral Johnson, Chief of Naval Operations*

In keeping with the Department of Defense (DoD) Joint Vision 2010, the Navy and Marine Corps have migrated to network centric methods for Command, Control, Communications, Intelligence, Surveillance, and Reconnaissance (C4ISR), control of logistical support, and administration. An inevitable consequence of this shift is that the ability of the Department of the Navy (DON) to conduct effective operations is increasingly network dependent. Disruption of information flow between deployed forces and supporting shore commands, joint service commands, or critical intelligence sources can significantly degrade situational awareness and the ability to coordinate operations in the tactical environment. DON networks, both classified and unclassified, are now mission essential combat enablers.

At the same time that network connectivity requirements have increased within DoD, efforts to re-engineer business processes and to improve morale and welfare within the Department of the Navy (DON) have necessitated additional connectivity between unclassified systems and the Internet (either directly or indirectly). These connections between public and DON networks provide obvious avenues of attack for adversaries, whether nation states or less conventional foes, which are accessible to anyone with a computer and a modem. Given the disproportionate network dependence of US forces, and the

availability of affordable computer access to public networks, network based information warfare could become the weapon of choice for our adversaries.

To counter this threat, DON needs to deploy an effective strategy (security architectures, policies, procedures, and tactics) for aggressive active computer network defense. Given the criticality of networks to its warfighting capability, DON network defense must be viewed as a defensive information warfare activity, rather than simply an information technology service. Similar to conventional combat, tactical command decisions on network defense will determine losses in operational capabilities, which in time of conflict could increase physical casualties. Appropriate strategies and tactics must be employed to preserve critical DON network assets.

In this paper we will describe a strategy for active defense of the Navy/Marine Corps Intranet (NMCI). The NMCI is a worldwide network connecting Navy and Marine forces at hundreds of locations around the world, at CONUS fixed shore sites. NMCI also connects these Naval forces to other DoD services and agencies, as well as contractors and suppliers on the Internet. We will attempt to demonstrate that effective defense of a network of this scope and complexity is a form of maneuver warfare spanning the entire lifecycle of the network.

## **2. The Threat Environment**

Defensive strategies are always constructed in response to a set of perceived threats. The threats facing the NMCI are the same well-publicized threats facing all DoD networks.

In times of war or lower intensity conflicts, there are the obvious threats of physical, or information warfare, attack from military opponents. Any military power is also a potential target for foreign intelligence services in times of peace or conflict.

However, given the expanding role of the Navy and Marine Corps in Operations Other Than War (OOTW), the sophistication of DoD technology, and readily available access to the Internet, DON networks are becoming more likely targets for asymmetric attacks from a number of less conventional sources. Among these asymmetric threats are terrorists, political activists/hacktivists, drug cartels, criminals engaged in industrial espionage, information warriors seeking to launch an attack on a third party from a DON network, and recreational hackers.

There are many potential sources, methods, and objectives for an attack against DON networks. See the table below for a few examples. An attack requires that an adversary have a vulnerability to exploit (either latent or inserted), an opportunity to access the system, and the skills/resources to exploit the

vulnerability. So, potential threats to the DON network can be derived from the table by selecting a threat source, one or more attack methods (usually at least one each for access, insertion, and exploitation), to achieve some number of objectives. Complex objectives are achieved by executing a sequence of attacks. The risk associated with each of these threats is determined by the probability that a particular threat source could acquire the necessary access, resources, and skills.

Threat Sources	Attack Methods	Attack Objectives
<ul style="list-style-type: none"> <li>• <b>Conventional Adversary</b> <ul style="list-style-type: none"> <li>- Military adversary</li> <li>- Foreign intelligence service</li> </ul> </li> <li>• <b>Unconventional Adversary</b> <ul style="list-style-type: none"> <li>- Terrorists</li> <li>- Political activist or hacktivist</li> <li>- Drug cartel</li> <li>- Criminal engaged in industrial espionage</li> <li>- Recreational hacker</li> </ul> </li> <li>• <b>Insider</b> <ul style="list-style-type: none"> <li>- Malicious user</li> <li>- Malicious developer or supplier</li> <li>- Uninformed user</li> <li>- User, developer, or supplier manipulated by outsider</li> </ul> </li> <li>• <b>Compromised Trusted Site</b></li> </ul>	<ul style="list-style-type: none"> <li>• <b>Gain Access</b> <ul style="list-style-type: none"> <li>- Collection of data on public network or RF</li> <li>- From public network</li> <li>- Malicious insider</li> <li>- Manipulated insider</li> <li>- Contacted by insider</li> <li>- Impersonation: stolen or exploited credentials</li> <li>- Clandestine access</li> <li>- Physical overrun</li> </ul> </li> <li>• <b>Insert</b> <ul style="list-style-type: none"> <li>- Nothing</li> <li>- Valid user credentials</li> <li>- Virus or malicious code (e.g. program, applet, or macro)</li> <li>- Software or hardware implant</li> <li>- Malformed or false data (spoofing &amp; rerouting)</li> <li>- Data observed from legitimate user (replay)</li> </ul> </li> <li>• <b>Exploit</b> <ul style="list-style-type: none"> <li>- Exploit security flaws in COTS product</li> <li>- Exploit security flaws in network protocols</li> <li>- Exploit security flaws in system</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• <b>Defeat Confidentiality</b> <ul style="list-style-type: none"> <li>- Eavesdropping</li> <li>- Cryptanalytic exploitation of data</li> <li>- Establish covert channel for extraction of data</li> </ul> </li> <li>• <b>Defeat Authentication</b> <ul style="list-style-type: none"> <li>- Impersonation of legitimate user using stolen or exploited keys</li> <li>- Acquire unauthorized privileges</li> <li>- Session or resource hijacking</li> <li>- Launch an IW attack on a third party from a US system (false flag)</li> </ul> </li> <li>• <b>Defeat Integrity</b> <ul style="list-style-type: none"> <li>- Modification of data or software (in transit or at rest)</li> <li>- Insertion of false data</li> </ul> </li> <li>• <b>Defeat Non-repudiation</b> <ul style="list-style-type: none"> <li>- Compromised audit logs</li> <li>- Compromised authentication keys</li> </ul> </li> <li>• <b>Defeat Availability</b> <ul style="list-style-type: none"> <li>- Destruction of data</li> <li>- Denial or disruption of network service</li> </ul> </li> </ul>

	<p>architecture</p> <ul style="list-style-type: none"> <li>- Perform cryptanalytic recovery of credentials or data keys</li> <li>- Exploit user or administrator configuration errors</li> <li>- Modify data, system configuration, software, or operating system</li> <li>- Destroy system or data</li> </ul>	<ul style="list-style-type: none"> <li>- Session or resource hijacking</li> <li>- Physical destruction of system</li> </ul>
--	--	---

Attacks can be launched from outside or inside the DON networks, depending on the access available to the attacker. However, the apparent source of an attack is not always a clear indication of when, where, or how the actual attack was executed. An attack that appears to originate from inside the DON network could actually be the consequence of a software or hardware change executed by an adversary before a particular component was delivered.

Inadvertent, or maliciously inserted, vulnerabilities can be introduced at any point in the lifecycle of the system and its components -- design, component implementation, system integration, distribution, installation, or user operation. Given the current state of COTS information technology, there are many ways for an adversary to manipulate a target system at the application, host, or network level. Some of the key reasons for this are described below.

*The rapid pace of change in network and information technology itself complicates the information assurance task. Fierce competition has accelerated product development cycles. As a result, neither industry nor government has the time or resources to perform extensive product testing, let alone extensive security vulnerability studies, on all COTS products before they are deployed. In many cases, even when security reviews are conducted, the product developer or evaluator does not have sufficient expertise to notice the vulnerabilities, which might be exploited by an expert in a particular attack method. The results are more rapidly acquired information technology, and more inherent risk, for government networks.*

## 2.1 Vulnerabilities of COTS Operating Systems and Software Applications

*Many COTS applications and operating system services were originally designed to run on an internal corporate network, not in a WAN environment. Often security was not a dominant factor in the selection of protocols, and authentication techniques tend to be based on exploitable password systems. Even in cases where security was a primary design consideration, new attack methods continue to emerge that make previous designs or implementations exploitable.*

*Vulnerabilities of COTS products (applications and operating systems) are routinely published on the Internet with sufficient technical detail to verify the vulnerability and to write an attack program, if one is not provided by an obliging researcher or hacker. Many of the same mechanisms which are meant to alert security professionals and system administrators to vulnerabilities of particular concern within a community (e.g. DOD), also inform hackers that the indicated attack will probably work against some of the machines in that community. Patches take time to deploy and often cannot be deployed without disrupting essential services. This provides a window of opportunity for the enterprising hacker.*

*Software implants and Trojan horses are also very serious threats to any security related program running on a general-purpose computer with network connectivity. Even high assurance operating systems cannot protect against malicious code embedded in the software installed by a system administrator, particularly if the code only effects its host program. Lower rated operating systems usually do not provide sufficient isolation of executing programs to prevent one routine from interfering with another, even if access controls prevent the stored target program itself from being modified.*

Even if the administrator properly configures a system, an implant may be able to alter security configurations as needed to accomplish its goals. Sophisticated implants can perform attacks normally associated with malicious insiders, and may be able to spawn processes with higher privileges than a typical user. Implants can employ sophisticated techniques to acquire system administrator privileges on many operating systems, if that is required.

Security programs can be subverted in sufficiently subtle ways that even a team of experts with complete knowledge of all inputs and outputs of the computer cannot detect the subversion, without completely reverse engineering the code. Key generation procedures can be manipulated, restricted information acquired and exfiltrated through covert channels, and files/programs changed or deleted (in motion or at rest).

*Trojan horses and implants can be found in shrink-wrapped COTS software as well as in viruses or programs (executable programs, Active X components, Java Applets, etc.) acquired over a network. In addition, the goal of a hacker may actually be to install a software implant, rather than to actively wander through a network.*

*The bottom line is that many software applications, operating system services, and LAN protocols either have latent vulnerabilities, or are subject to manipulation by a skilled adversary. And there are a number of methods for an adversary to accomplish a system modification. (See the previous threat table.) Essential services for communication with contractors on the Internet, such as e-mail and web services, are common vehicles for launching attacks.*

## 2.2 Vulnerabilities of COTS Networking Devices

*Many COTS networking devices and protocols also have significant security problems.* Products compliant with existing standards use only weak authentication for critical inter-device signaling. For example, ATM signaling (UNI, PNNI, NNI), IP routing protocol updates, Domain Name Server (DNS), and remote management protocols (e.g. SNMP, telnet, etc.) can all be spoofed or exploited with replay attacks. So, signaling flow can be blocked, redirected, or delayed to deny network service to a target. Although industry standards bodies have proposed more secure alternatives to some of these protocols, product developers have been slow to update products. Even with the improved protocols, particular product implementations may also suffer from more subtle security flaws.

## 2.3 Minimizing Threats to NMCI

An adversary with access to the NMCI, or even the ability to provide a program for execution on an NMCI computer, can launch a number of attacks against COTS applications, operating systems, and networking components. Although the precise vulnerabilities and attacks will vary over time, it is prudent to design the NMCI with the assumption that there will be exploitable vulnerabilities in the network, particularly at the individual host or local area network (LAN) level. An obvious conclusion is that we must limit the ability of an external adversary to access, or provide malicious content to the NMCI. Interoperability requirements with the rest of DoD and contractors on the Internet prevent perfect isolation of the NMCI from external threats. All that we can do is minimize the number of protocols and paths that can be used to attack the NMCI from the outside. In addition, we must carefully monitor what flows into the NMCI, block what is clearly dangerous, and respond as quickly as possible to what seemed to be benign but was not.

*We have tried to quickly summarize the nature of the threats to the NMCI. With this as background, we shall now explore strategies for defending the DON networks. Given the diversity of threats, the rapid change of information technology, and continually evolving attack methods, perfect network defense will remain elusive. But technologies, procedures, strategies, and tactics can be applied to minimize both the probability of, and the damage to critical systems in the event of, a successful attack. A key element of a successful strategy for defense of the NMCI is to view network defense as a form of cyber maneuver warfare.*

### **3. Useful Analogies: Defensive Systems for Modern Warships and Tactics for Battlegroups**

To illustrate the essential elements of a strategy for active defense of DON computer networks in a more tangible context, let us consider the integrated defensive systems that protect a modern warship.

A modern warship's defenses begin with the design of the ship's hull. The hull of the ship is covered with armored plating to harden it against penetration (in case of physical attack or accidental collision). Since there are known weapons and accidents that can penetrate this armor, the hull of the ship is divided into watertight compartments connected by hatches. If the armored hull is compromised, the breached compartments are identified and appropriate hatches are closed to isolate the effected compartments behind watertight barriers. This prevents a compromise in one compartment from flooding the entire ship and minimizes water damage to ship's systems.

Other shipboard systems attempt to reduce the probability that the hull is ever compromised. Accurate navigation methods, radar, and sonar systems reduce the probability that the ship will run aground. Radar, sonar, and IFF systems attempt to identify hostile forces or weapons approaching the ship. Ship missile defenses attempt to intercept a surface or air threat as far away from the ship as possible (to limit the ability of the attacker to inflict damage) and point defense

systems on the deck attempt to shoot down any threat which penetrates the missile defense system.

Battlegroup tactics further protect the most vital ships by deploying a variety of screening aircraft, submarines, anti-submarine helicopters, and escort ships in layers around the carrier, Amphibious Readiness Group, and other priority ships. All of these defensive mechanisms (on individual platforms and combined tactics) form an integrated system for protecting the battlegroup, but not all battlegroup assets are protected equally. The defenses native to the battlegroup are also augmented by support from other services in a combined operation, and by externally provided intelligence providing threat warnings and situational awareness.

The notion of applying layered defenses around high valued assets is known as "Defense in Depth". The idea is to deal with threats as far away from critical assets as possible to enable time for alternative measures to be applied if initial efforts fail. The number of layers protecting any individual asset is then balanced against its intrinsic value to conduct operations.

The layered defensive systems described above need to be actively manned by skilled personnel, under effective local and national DON leadership to maximize defensive effectiveness. DON activities must also be closely coordinated with theater and global Joint Service, and other US government, assets to maximize effectiveness of the overall DoD defensive strategy and to conduct larger operations.

Many of the tactics and strategies used to increase survivability of Naval forces against physical damage (in war, operations other than war, and sustaining operations) also have analogs in the cyber world. These concepts form the foundation for an active computer network defense strategy.

#### **4. Mapping the Analogies to the Network World**

##### **4.1 The Warship Analogy:**

We will first derive network defense concepts from the analogy of the individual warship. The first step is to harden the boundary separating DON networks from the Internet, as well as from other DOD unclassified and classified networks. This outer boundary plays the role of an armored ship's hull. Defensive resources must be applied to minimize the probability that this outer boundary is penetrated or compromised. All classified systems must be separate from unclassified systems by NSA approved high assurance encryption and guard devices.

However, DON has extensive requirements for data exchange with contractors on the Internet, DOD unclassified systems on the NIPRNet (Non-Classified Internet Protocol Routing Network), and DOD classified systems on the SIPRNet (Secret Internet Protocol Routing Network), which also must be accommodated by the outer boundary defenses. The strategy is to apply a variety of COTS network security technologies within each classification level at the outer boundary (similar to the missile and point weapon systems on a ship) to minimize the probability that the outer boundary is penetrated. But, there are known methods for penetrating either the data protocols that must be allowed through the outer perimeter, or the perimeter COTS security products themselves.

Since we know that the DON network "hull" can be compromised with sufficient expertise, we must apply other strategies to isolate and minimize the impact of a penetration. Similar to a warship, the DON network should be divided into geographic compartments (regional, base, and/or command level), each with the mechanisms and procedures to detect boundary or internal compromises, and to seal themselves off from other compromised compartments. These individual compartments collectively form a sensor grid and active response system for the entire DON network. The local vulnerability detection mechanisms of compartments of the DON network will also be supplemented by red team (government vulnerability assessment team) support from DON and other DOD agencies (e.g. NSA and/or DISA).

#### 4.2 The Battlegroup Analogy:

From the Battlegroup analogy, we derive additional network defense tactics. Network assets must be prioritized in terms of criticality to supporting warfighting capabilities. Although a single layer of defense may be adequate to protect DON administrative functions, additional layers are essential to adequately protect combat and combat support functions. Layered, diverse defenses maximize the probability that threats will be detected and blocked as far away from critical assets as possible, and enable time for alternative measures to be applied if initial efforts fail. Usually attacks which penetrate the outer boundary, even if they are isolated and counteracted, require clean up and restoration operations that can be disruptive. In time of crisis, these restoration activities should be done somewhere other than an essential command for combat operations, if it can be avoided.

As in the battlegroup scenario, DON network defense efforts will be augmented by support from other DOD services and agencies, some of which was described above. An additional element of this support is intelligence received from

external sources providing threat warnings and situational awareness. The severity of the current perceived IW threat will be communicated as an Information Operations Condition (INFOCON level). Based on the INFOCON level, steps must be taken to reduce the exposure of operationally essential commands to cyber threats. (The detailed requirements are classified.) At the same time, the normal business of non-tactical and support commands, which may require freer access outside of DON, cannot be impeded in the absence of an actual cyber threat. So, the security architecture of the DON network must allow designated commands, and logical communities of interest which may be geographically dispersed, to further isolate themselves from the rest of the DON network in response to increased INFOCON levels. Since these are the same commands that should be defended by multiple layers (as described above), a common approach can be developed to satisfy both security requirements.

The battlegroup defense analogy also suggests that the interactions between defensive systems, procedures, and tactics are critical to effective defense of a complex system. The critical elements of information assurance are summarized by the following words: Protect, Detect, React, Recover and Revise. The specific required capabilities for each of these elements, and their interactions, are described in subsequent sections.

## **5. Protect: Deploying Screening Forces and Force Concentrations**

The first phase of an active CND strategy, Protect, is focused on initial deployment of the elements associated with network defense in depth. A diverse set of complementary network defense technologies is deployed in parallel layers based on the concept of risk minimization. The number of layers protecting any given asset is determined by its criticality to supporting warfighting capabilities. We will first address natural boundary layers (logical or physical) within the DON network, then the types of network security technologies which should be deployed at each layer, and infrastructure hardening which must occur throughout the NMCI.

### **5.1 Separation of Classification Levels**

The first mandatory boundary to establish is between systems operating at different classification levels. As required by national policy (DODD C-5200.5), all U.S. classified information must be protected with National Security Agency (NSA) approved high-grade cryptography. DOD policy (DOD 5200.28) also states that all DOD information systems and networks (classified as well as unclassified) shall be subject to a certification and accreditation (C&A) process which verifies the required levels of information assurance are achieved. In addition to separating data at different classification levels, the system must be designed so that the reliability and availability of a classified system cannot be

effected by unclassified systems. This usually implies that separate infrastructures are needed for classified and unclassified networks, and only approved high assurance guards are allowed to transfer data between classification levels. This approach is referred to as Multiple Security Levels (MSLs). There are two formal mechanisms to insure proper separation for classified infrastructures. The Defense Information Switched Network (DISN) Security Accreditation Working Group (DSAWG) has final approval authority before any system is connected to the SIPRNet. Also, any device that is used to provide connectivity between Secret and unclassified networks must be in accordance with the guidelines established by the Secret and Below Interoperability (SABI) process.

It is important to note that although the degree of implementation may vary for protection of classified infrastructures on the SIPRNet and unclassified infrastructures, a defense in depth strategy is required in both environments. Because the SIPRNet is the primary operational network during both peacetime and war for the Department of Defense (DOD), there is potential for significant damage if network penetrations occur. Scenarios such as physical overrun of a network node and malicious insiders need to be considered.

All subsequent discussion in this section will focus on providing layers of defense within a particular classification level. Commercial off the Shelf (COTS) security products, that meet appropriate DON IA guidelines, can be used within a classification level. Within a classification level, a risk management approach is used to balance the level of containment against fiscal reality.

## 5.2 Logical Boundaries within a Classification Level

As indicated in section 2.3, an adversary with access to the NMCI, or even the ability to provide a program for execution on an NMCI computer, can launch a number of attacks against COTS applications, operating systems, and networking components. Within each classification level a number of logical security boundaries, some mandatory and some implemented as required, need to be established and defended to shield mission critical LAN's from external or internal attack.

Boundary 1: Logical Boundary between NMCI and External Networks  
Boundary 2: Logical Communities of Interest within DON Network (as required)  
Boundary 3: Local Area Network (LAN) and/or Base Area Network (BAN) (as required)  
Final Layer of Defense: Application/Host Level

The number of layers of defense protecting any given network node will depend on its physical placement within the NMCI network architecture, its criticality to supporting warfighting capabilities, and restrictions on the data or protocols at the node. Let us consider each possible boundary in additional detail. Appendix Three provides notional concepts of security relevant designs.

### Boundary 1: Logical Boundary between NMCI and External Networks

The first mandatory defensive boundary consists of all points of connectivity between NMCI controlled network assets and external networks (e.g. the Internet, NIPRNet, or SIPRNet). Boundary 1 forms the “armored hull” which reduces the probability that an external adversary will penetrate the NMCI. Subsequent boundary layers will play the role of the watertight compartments in the hull of a warship, isolating penetrations while providing maximum protection to vital NMCI assets.

A primary purpose for Boundary 1 is to deny an adversary access to insecure protocols and applications that might be required for general DON internal use. Boundary 1 also acts as the outer screening force for the NMCI, countering lower grade threats and providing early warning of more severe threats requiring defensive maneuvers. As such, commands protected only by boundary 1 will tend to absorb the most damage. A well-constructed perimeter defense should enable more rapid adoption of new technology within the NMCI, since risks associated with less evaluated technologies and emergent attacks are managed.

However, interoperability requirements between NMCI and external networks (Internet, NIPRNet, and SIPRNet) will determine how watertight this boundary can be. Every effort must be made to minimize the number of insecure protocols allowed through the outer perimeter. Standard DON policies, architectures, and procedures are critical on boundary 1 because the integrity of the “hull” will be determined by its weakest point. Encrypted sessions between NMCI and non-NMCI sites through this boundary must also be carefully managed to insure that the encrypted channels are not being utilized to tunnel through outer defenses. Ideally, the contents of every path through boundary 1, whether encrypted or not, would be covered by at least intrusion detection and content filtering.

Boundary 1 is also the perimeter separating trusted NMCI networking components from less trusted external networks. Particular attention must be given to hardening the network infrastructure at this boundary (DNS, NTS, network management, etc.) to resist denial of service attacks launched from the untrusted network.

Depending on the eventual network topology for the NMCI, logical boundary 1 could be implemented at a regional NMCI MAN, BAN, or LAN connection to an external network. Regional enforcement allows one site to take actions to screen an entire region from external network threats, or threats originated from another region/location on the

NMCI. Connections between two NMCI nodes behind boundary 1 must be carefully handled with hardened NMCI links and/or appropriately encrypted links over external networks to insure that the boundary is not compromised.

*Boundary 2: Logical Communities of Interest within DON Network (as required)*

Logical boundary 2 is an optional perimeter that separates a logical community of interest within the NMCI from the general DON population. Many of these communities of interest involve geographically dispersed elements which exchange restricted access information (or protocols), or require the ability to enforce a tighter policy than can be enforced at boundary 1 (particularly in times of crisis or increased INFOCON level). The following are a few examples of DON logical communities of interest.

- Personnel system – Privacy Act Data
- A major claimant (USN or USMC) which is geographically dispersed
- Commands and shipyards handling nuclear propulsion data
- Commands requiring access to the DoD Joint C4ISR system
- Elements requiring access to NMCI network management and network defense systems

All command elements involved in a coalition operation (US and allied) - only required information shared

*Boundary 3: Local Area Network (LAN) and/or Base Area Network (BAN) (as required)*

Boundary 3 provides an additional layer of defense that can be applied at the natural LAN and/or BAN boundaries. LANs or BANs provide natural physical boundaries that can be used divide the NMCI into watertight compartments within the outer perimeter. At boundary 3, penetrations from the outside can be limited, and attacks originating from the LAN/BAN network can be contained. The attacks originating from the LAN/BAN network can either be launched by an insider, or be the indirect actions of an outsider. The policies implemented at boundary 3 can be more restrictive than at boundaries 1 and 2 since smaller, more distinct communities of interest are addressed. An example would be the BAN providing network services for the North Island Naval complex within San Diego, where multiple commands within a close geographical proximity could be defended as a unit.

Final Layer of Defense: Application/Host Level

Application and host level defenses are the last layer of defense in depth. At the host workstation level, the emphasis is on securely configured and configured operating systems and application software. As indicated in section 2, there are

challenges associated with defending COTS software based systems. But, tightly configured operating systems with the latest patches, and no unnecessary services installed, significantly complicate attacks. Tightly designed and configured applications also minimize threat potential. Virus/content filtering software and other host based defenses (PKI enabled applications, secure e-mail, SSL, file encryption, etc.) also minimize threats at the host or application level.

## Understanding the Relationship of the Boundary Layers to Active Defense

Application and host level security are the last line of defense separating an adversary from operational data and resources. Of course, some application protocols must be allowed to pass through all layers of defense to enable interoperability with other elements of DoD or contractors on the Internet. As discussed in section 2, there are known ways to exploit some of these required protocols and the data passed through them. These known gaps through all layers of NMCI network defense are similar to gaps in zones of fire given the way conventional forces are deployed. Gaps are always areas for reconnaissance and maneuver warfare, since they are the paths of least resistance for enemy assaults.

The existence of these required protocol gaps necessitates layered defenses for mission essential commands. In order to minimize exposure in times of increased threat, a mission essential community of interest may decide to close some of the gaps that would normally be open. Other commands requiring freer access to external networks may not be able to function properly without all normal protocols to communicate. Providing a boundary 2 defensive layer around the mission essential community allows it to independently enforce a stricter policy.

Boundaries 1, 2, and 3 described above enable enforcement of a DON three-layer protocol and data access policy. A particular community of interest could enforce a stricter policy than that required by DON.

Layer 0: DMZ

Layer 1: DON to/from Anyone

Layer 2: DON General Internal Use

Layer 3: DON Restricted Use or Community of Interest Restricted Use

Layer 4: DON Restricted Use or Community of Interest Restricted Use with VPN support

Layer 5: Host/Application

## 5.3 Component Security Technologies

In this section, we will briefly describe a few of the security technologies that can be used to construct the boundary layer defenses described above. None of these technologies is a complete solution, but an integrated approach can be quite effective.

## Firewalls and Packet Filtering

Firewalls perform rule-based filtering on data packets based on some combination of packet structure, header contents (TCP/IP ports, source and destination IP addresses, etc.), and packet sequence. The more sophisticated variants proxy particular services and/or make intelligent decisions based on the protocols associated with specific applications. Firewalls are used to control the protocols allowed to pass through a boundary and to block certain attacks based on maliciously constructed packets. (e.g. Allow web sessions originated from inside the firewall, but not sessions originated from outside the firewall.) However, firewalls usually do not evaluate the contents of packet payloads.

For each application operating across a firewall perimeter, accommodations must be made in the firewall for all TCP/IP ports required by the application. Given the geographic dispersion of the Navy and Marine Corp, many DON internal applications transit firewall perimeters. Since many of these applications (COTS and GOTS) were not designed with protocol security in mind, and the complexity of the IP address space complicates restrictions by IP address, dangerous protocols often are allowed to pass through DON firewalls. (The Marine Corps has maintained more consistent firewall discipline than the Navy.) So, firewalls in isolation are not effective perimeter defenses for DON networks. (This was one of the primary motivations for the conceptual security architecture described in Appendix 3.)

## Intrusion Detection

Intrusion detection systems look for patterns of activity or statistical anomalies in network traffic that match known attack profiles. But, they only detect attacks matching their preset profiles, and then often incorrectly label legitimate network traffic as an attack.

Although many of these devices can be programmed to automatically respond to an observed attack, active shunting is not practical in DoD networks because of legal constraints against unauthorized counterattacks and risk of self-inflicted denial of service.

In passive mode, IDS systems are merely warning systems indicating that certain types of network attacks are underway. An attack not matching existing profiles, or in encrypted network traffic, will not be alarmed.

### Content Filtering: Virus and Malicious Code

Content filtering products scan files and programs for signatures corresponding to known viruses, known malicious code, or pre-defined word patterns. They can be also programmed to take corrective action when the pattern is identified. Similar to IDS devices, content filtering programs only search for known signatures. Other mechanisms are required to identify the unusual activity associated with a new virus or malicious file. Of course, these mechanisms do not work on encrypted files.

### *VPN Encryption & SSL Session Security (Authentication, Confidentiality, and Integrity)*

Virtual Private Network (VPN) packet level encryption devices provide confidentiality, authentication, and integrity protection for securely connecting networks, or for secure remote access, over a public network. These devices are frequently used in DON networks to cryptographically separate communities of interest, protect restricted data on public networks, and as containment fields (via tunneling) for applications using dangerous protocols.

However, VPN devices must be carefully integrated into an overall network security architecture, because encryption and packet tunneling nullify the effects of firewalls, intrusion detection systems, and content filtering mechanisms. From a security perspective, two networks connected by VPN encryption should be evaluated as a single network, ignoring all other security mechanisms between the two networks.

Secure Sockets Layer (SSL) is a protocol that performs similar functions in a client – server environment. It is commonly used within DON for security of web traffic and other applications. If a host is connected to a server via SSL, then all content filtering mechanisms between the two machines are ineffective because the session is encrypted. SSL is standard in all web browsers and the remote server determines whether it is used. This can be problematic if a DON user visits a malicious web site on the public Internet.

### DoD Public Key Infrastructure Enabled Applications

Public key cryptography will be broadly utilized throughout DoD for authentication (web, network, and physical access), digital signatures, and secure e-mail in the next two years. By DoD policy, all DoD services and agencies are

required to use only the official public key infrastructures authorized by NSA – currently the high assurance PKI based on FORTEZZA and the medium assurance PKI based on X.509v3 certificates. All DoD PKI applications will be required to use NSA authorized cryptographic hardware tokens, reference Statement of Objectives, section 6.2.

All PKI enabled applications for the NMCI must be compatible with the DoD PKI, and authorized DOD certificate authorities must issue all certificates. Use of DoD PKI will be mandatory security of private web servers and signed e-mail (according to timelines specified by DoD policy).

### Utilizing the Components in an Integrated Security System

All of the security technologies described above make complementary contributions to the security of the DON networks within a classification level. An effective security solution for the NMCI will require effective integration all of these technologies, as well as approved solutions for separation of classification levels. (See section 5.1.)

There are many possible methods for combining the security components above to enable implementation of the active defensive strategy described in this paper. (See Appendix 3 for one example security architecture.) Many tradeoffs can be made between cost, scalability, strength, and depth of defense.

Although DON does not intend to impose a specific security architecture upon the NMCI, designated DON staff must approve the actual security architecture implemented for the NMCI. All security critical products utilized in the architecture must also be approved

### 5.4 Infrastructure Hardening

As mandated in Presidential Decision Directive 63, appropriate measures must be taken to provide protection for the nation's critical infrastructure. Correspondingly, throughout the NMCI network infrastructure hardening must be addressed. Specifically, strong, non-spoofable access control mechanisms need to be implemented for managed devices (routers, servers, switches, etc.). Strong authentication (PKI enabled or keyed hash) and network encryption can be used to counteract some threats. Vulnerable switch signaling can be protected by out of band management or VPN tunneling, and authenticated routing protocol updates can be implemented using keyed MD5 (or VPN). DNS can also be hardened with host protections or by the evolution to the DNS Security (DNSSec) standard. Network or enterprise management tools can used to

continuously monitor the status and security of the network to improve the reaction time in the event of denial of service attack.

The NMCI network must also have sufficient redundancy and geographically dispersed paths to survive physical attacks or natural disasters.

We have described at least the key portions of the Protect phase of an active computer network defense strategy. In the Protect phase, the emphasis is on deploying diverse security technologies and architectures to block as many avenues of attack as possible (given reality constraints), to add depth to the defense, and to provide warning of as many known attacks as possible on attack vectors that cannot be blocked (given requirements for interoperability and the deployment of defenses).

## **6. Detect: Extended Reconnaissance for Opposition Forces and Vulnerabilities**

The Detect phase of active defense involves vigilant reconnaissance for attacks (penetrations, exploitations, or loss of capabilities) against known gaps in NMCI defenses, and a search for previously undiscovered NMCI vulnerabilities. It is prudent to assume that an adversary with sufficient expertise, resources, and access will penetrate NMCI boundaries.

In the Protect phase, sensors were deployed strategically within a sensor grid providing regional and local coverage. In the Detect phase, attack sensor systems and security relevant audit logs are actively monitored for signs of attack. Because of the current limitations of current sensors, all attacks will not be indicated by individual sensor outputs. Additional indications of attacks are derived from correlation and synthesis of data across different types of sensors, geographically dispersed sensors of the same type, time, and other parameters. It is also critical to be able to distinguish probable attacks from false positives, when there are both benign and malicious interpretations of network events.

Network availability, security sensor information, and validated attacks from each local area and region must be made available to the DON components of the DOD Joint Task Force for Computer Network Defense (JTF-CND), so that analysis can be performed across regions and network defensive strategies coordinated across DON. The DON components of JTF-CND will work with the other elements of JTF-CND to coordinate network defense across DOD and the US Government as a whole. Similar information must also be provided by appropriate DON commands to DON regional Fleet Commander in Chiefs (FLTCINCs), so that regional network defense can be coordinated and integrated more effectively with Joint Service regional CINCs.

Indications of attack, significant vulnerabilities, or warnings of increased threats from other elements of the federal government (DoD, the intelligence community, FBI, or other federal agencies) will also flow from DON components of the JTF-CND to the NMCI. For example, Information Assurance Vulnerability Alert (IAVA) notices are disseminated from DISA outlining known vulnerabilities within products and/or recent intruder information. The Information Operations Condition (INFOCON) is another method for quickly conveying the severity of perceived threats against DoD networks. Designated DON personnel will have authority to direct NMCI activities in response to actual attacks or perceived threats.

Other detection activities focus on identifying unobserved vulnerabilities in the NMCI. Vulnerability scanning tools should be used to detect improperly configured security critical components. Network mapping and analysis tools can be used to search for unauthorized connections between the NMCI and external networks.

NMCI internal vulnerability detection efforts will also be supplemented by independent red teaming efforts approved by DON. In particular, DON red teams (supported by NSA, DISA, or other federal agencies) will security architectures, security product selection, and fielded NMCI configurations for latent vulnerabilities (either previously undiscovered, recently inserted, or resulting from emergent attacks). DON red teams will also performed authorized and controlled attacks on actual NMCI networks to test fielded configurations. Red teaming is a normal part of DON quality control and continual improvement processes.

## **7. React: Maneuvering to Repulse Opposition**

Once a successful attack has penetrated the NMCI, the perceived threat against the NMCI has significantly changed (e.g. INFOCON level has increased), or a latent vulnerability has been detected in the NMCI, appropriate countermeasures must be taken.

In the event of an actual penetration (intrusion or malicious code), the layered defenses within the NMCI should be used to identify and to isolate the effected portions of the NMCI rapidly. However, these defensive actions may result in denial of some or all services for subnets of the NMCI. The particular tactical approach taken (sequence of actions, effected commands, and effected services) could have significant impact on critical, ongoing Navy and Marine Corps operations. The objective of the adversary may be simply to coax DON into over reacting to a cyber attack in order to degrade the capabilities of operational forces.

Therefore, these network attack response decisions constitute IW defense command decisions that must at least be authorized by designated, uniformed DON personnel knowledgeable about ongoing operations and subtle relationships between DON commands. The DON command structure must retain directive authority over all NMCI threat responses. These DON personnel will also be the conduits for authorized responses to directives received from JTF-CND, or Joint Service regional CINCs, for coordinated joint service responses to threats. These Joint Service directives must also be interpreted in light of ongoing DON operations. Similarly, DON personnel must approve responses to latent vulnerabilities and configuration errors to avoid unintended adverse impacts.

It is anticipated that the ongoing dialogue between the DON military command structure and NMCI personnel will be mutually beneficial. Both the NMCI architecture and DON defensive IW strategies/tactics should improve over time. In less time sensitive scenarios, cost benefit tradeoffs will need to be considered and mutually acceptable implementations agreed upon.

Although automated responses to some attacks might appear attractive at first glance, they must be carefully reviewed prior to implementation. Both legal and operational constraints must be considered. According to current Department of Justice interpretation of US law, the inherent right of self-defense of US military forces does not extend to a right of counterattack in the event of cyber attack. Until sufficient counter evidence is collected, all cyber attacks are considered criminal matters, because they could have been initiated by a US person, even if they appear to come from a foreign site. (It is a common practice to launch cyber attacks from previously compromised machines to source determination more difficult.) Even active probes to determine the actual source of an attack that extend beyond DON (or possibly DoD) networks might be considered "attacks" by NMCI personnel on intermediate machines. Current US law on computer security only makes exceptions for authorized FBI law enforcement, and intelligence community foreign intelligence collection, activities.

There are also operational considerations that argue against aggressive automated responses. If a sensor incorrectly identifies legitimate network activity as an attack (not an uncommon even for some current sensors), the result of an automated response could be cyber fratricide. Moreover, given the practice of launching attacks from previously compromised machines (i.e. false flag operations), the apparent source of an attack may be deceptive.

Standard NMCI response activities must be restricted to preventing, isolating, terminating, and determining the apparent source of attacks within the

boundaries of the NMCI. These activities must be carefully coordinated with the DON components of JTF-CND, which will coordinate as necessary with other elements of DoD, FBI, the intelligence community, and other federal agencies to trace the attack beyond the boundaries of the NMCI and to coordinate appropriate counterattack measures, if any.

## **8. Recover & Revise: Consolidating Forces and Re-establishing a Perimeter**

We will now consider the final phase of network defense Protect – Detect – React – Recover & Revise cycle. Once an attack has been terminated, systems and data effected by the penetration must be restored to their operational condition prior to the attack (to the greatest extent possible).

A damage assessment is also a critical after action activity to determine what was compromised, what could not be recovered, what commands were effected, and duration of outages. The nature of the attack and the defensive actions of the NMCI team also should be reviewed to determine whether changes should be in the network configuration, security architecture, products, product configurations, or procedures/tactics/doctrine/training. In this analysis phase, it is critical to determine whether new attack methods were used and whether there are attack signatures that could be used to update systems to prevent or to detect similar attacks in the future. All of the above recommendations should be prioritized and cost/benefit tradeoffs considered.

The recovery and revision process can be costly in terms of time and manpower, so maximum benefit must be derived from lessons learned from actual, or simulate red teaming, attacks. Due to the intensive manpower required for recovery and revision operations, it is essential that the overall NMCI security architecture provide maximum protection for mission critical operational and support commands. To accomplish this goal, the NMCI must employ layered defenses and appropriate response tactics.

## **9. NMCI: Critical Government Roles**

Although DON intends to pursue an aggressive outsourcing strategy for design, deployment, and operation of the NMCI, authorized DON personnel must perform a number of security critical roles. These roles fall into two categories: insuring that the security of the NMCI satisfies DON, DOD, and federal requirements, and exercising essential command authority over DON defensive IW activities.

In keeping with the Certification and Accreditation required for all DoD computer networks (classified and unclassified), authorized DON personnel must approve the security architecture, security critical product selections, the network connectivity plan, security procedures, and other security critical factors of the NMCI. DON personnel will seek to use the most expeditious procedures that do not compromise the integrity of the security evaluation process.

DON red teaming in the form of design, product, and configuration reviews, as well as authorized simulated attacks against operational NMCI networks, will be a primary tool for insuring that the NMCI satisfies DON and DoD security requirements. DON will seek assistance from NSA and DISA in these red teaming efforts, to insure that DoD concerns are addressed.

As discussed in section 7, responses to network threats and attacks constitute IW defense command decisions that must at least be authorized by designated, uniformed DON personnel knowledgeable about ongoing operations and subtle relationships between DON commands. The DON command structure must retain directive authority over all NMCI threat responses. These DON personnel will also be the conduits for authorized responses to directives received from JTF-CND, or Joint Service regional CINCs, for coordinated joint service responses to threats.

Network availability and security sensor information from the entire NMCI must be made available to the DON components of the DOD Joint Task Force for Computer Network Defense (JTF-CND), so that analysis can be performed across regions and network defensive strategies coordinated across DON. The DON components of JTF-CND will work with the other elements of JTF-CND to coordinate network defense across DOD and the US Government as a whole. Similar information must also be provided by appropriate DON commands to DON regional Fleet Commander in Chiefs (FLTCINCs), so that regional network defense can be coordinated and integrated more effectively with Joint Service regional CINCs.

The level of government oversight, approval, inspection, and qualification authority over the NMCI design and implementation process suggested above is similar to the methodology used in the aggressive outsourcing approach used by the DON for the design and construction of warships.

However, the operational control over the NMCI is actually significantly less than that applied to operational warships. In spite of the fact that the NMCI must be viewed as an IW defense platform, much of the NMCI will be owned and operated by industry. DON personnel retain only essential command authority and approval of security significant changes.

## **10. Conclusions**

Technology alone is not sufficient to address the network security challenges of the NMCI. Effective active computer network defense is a full life cycle process involving technology, intelligent system design, proper system configuration

and administration, procedures, skilled personnel, effective leadership, defensive strategies, cyber maneuver tactics, and coordination with the military command structure. In other words, defense in an information warfare context looks much like defense in conventional warfare contexts. The many lessons learned by the Navy and Marine Corps in conventional warfare need to be examined for applicability to cyber warfare. NMCI active network defense is not something which should be left entirely to civilian IT professionals, whether they are contractor or government. Some of the decisions involved should be considered IW-Defense command decisions, which require appropriate authority for risk assumption.



## **Appendix 1: DOD & DON IA Policies & Instructions**

### **General INFOSEC**

- SECNAVINST 5239.3 dtd 14 Jul 95: DON Information Systems Security (INFOSEC) Program
- DOD 5200.1 dtd Jan 97: DOD Information Security Program
- DOD 5200.28 dtd 21 Mar 88: Security Requirements for Automated Information Systems (AISs)
- DON CIO Information Technology Standards Guidance (ITSG) Version 99-1 dtd 5 Apr 99
- CNO N6 ALCOM 081949Z SEP 99 Protecting Unclassified Networks from External Threats
- USMC CIO IA Policy
- OPNAVINST 5239.1B
- DoD CIO Guidance Memorandums on Information Assurance (IA) 6-8510

### **Certification and Accreditation (C&A)**

- DODD 5000.1 Major Systems Acquisition
- DODD 5000.2-R Major Systems Acquisition
- DOD IA8500-L Information Assurance Requirements
- DOD 5200.40 dtd 30 Dec 97 DOD Information Technology Security Certification and Accreditation Process (DITSCAP)

### **Information Warfare**

- DOD INST 3600.1,
- Joint Pub 3-13 dtd 9 Oct 98, Joint Doctrine for Information Operations
- C-JCSI 6510.01b dtd 22 Aug 97, Defensive Information Operations Implementation
- OPNAVINST 3430.26 dtd 18 Jan 95, Implementing Instruction for Information Warfare/Command and Control Warfare

### **Support for Coalition Operations**

- JP 3-0 dtd 1 Feb 95, Doctrine for Joint Operations

### **NATO**

- Ad Hoc Coalition

### **CND**

- OPNAVINST 2201.2 dtd 3 Mar 98, Navy and Marine Corps Computer Network Incident Response
- MARFOR CND Security Concept of Operations
- MARFOR CND Security Policy and Guidelines
- Message DTG R181840Z dtd May 99 Navy Information Operations Condition (INFOCON) Implementation

- CJCS Memo CM-510-99 dtd 10 Mar 99, DOD INFOCON Guidance
- Draft NCTF-CND Concept of Operations (CONOPS) dtd 29 Jan 99
- CNO Message DTG R 211417Z Oct 98, Information Assurance Vulnerability Alert (IAVA) Process
- CNO Message DTG R071310Z Jul 99, Change of Information Assurance Vulnerability Alert (IAVA) Reporting Agent
- MARFOR IAVA Process

### **DOD PKI**

- DEPSECDEF Memo dtd 09 Apr 1999, DOD PKI Implementation

### **Web Security**

- DEPSECDEF Memo dtd 7 Dec 99, Web Site Administration, Policies & Procedures
- DEPSECDEF Memo dtd 24 Sept 98, Information Vulnerability and the World Wide Web
- OSD Memo dtd 9 Jan 98, Policy for establishing and maintaining a publicly accessible Department of Defense Web Information Service
- CNO Message DTG P 232300Z Oct 98, Navy World Wide Web Policy Execution
- CNO Message DTG R 140100Z Nov 98, Waiver Request to Navy World Wide Web
- IA Training and Certification joint memo dated 29 June 1998, from Under Secretary of Defense (Personnel and Readiness) and Assistant SECDEF for C3I
- SECNAVINST 5720.47 on DoN Policy for Content of Web Sites

### **Policy**

- CNO Message DTG R 261622Z Mar 99, Navy World Wide Web Monitoring DoD Interoperability
- Joint Doctrine Capstone and Keystone Primer dtd 15 Jul 97
- JP 1 dtd 10 Jan 95, Joint Warfare of the Armed Forces of the United States
- JP 1-01 c1 dtd 14 Sept 93, Joint Publications System, Joint Doctrine and Joint Tactics, Techniques and Procedures Development Program

## Appendix 2: Defense Against Example Attack Scenarios:

Detect, React, Restore functions in network world equivalent to ship's crew operations in conventional world. Command decisions required. Scenarios to clarify all of the above points.

Virus or Malicious Code Infection:

NIPRNet: introduced by mail from Internet, brought in by employee, contained in authorized COTS software but not detected prior to or at install, brought back in encrypted session (e.g. SSL) from Internet, etc.

SIPRNet: introduced by unauthorized load by insider (DoD or contractor), contained in authorized COTS product but not detected prior to or at install, HAG system failed to detect on write up from unclassified to classified network

Coalition:

Network Intrusion:

NIPRNet

Outsider:

- Uses vulnerability in standard protocol allowed through boundary defenses to gain access or insert malicious code
- Uses flaw (inadvertent or inserted) in COTS security products (architecture defect, authentication defect, legacy code, encryption flaw yielding authenticating information, trap door, etc) to gain access or insert malicious code directly or indirectly
- Theft of authenticating information enabling impersonation of authorized user
- Session or resource highjacking

Insider:

- Unsophisticated direct attack by insider
- Use of flaw in COTS product or protocol used behind firewall to gain additional access or insert malicious code

SIPRNet:

Penetration of Type 1 boundary defenses required to initiate an attack

Outsider:

- Theft of keying material or recruitment of insider to

Denial of Service or Disruption Attack

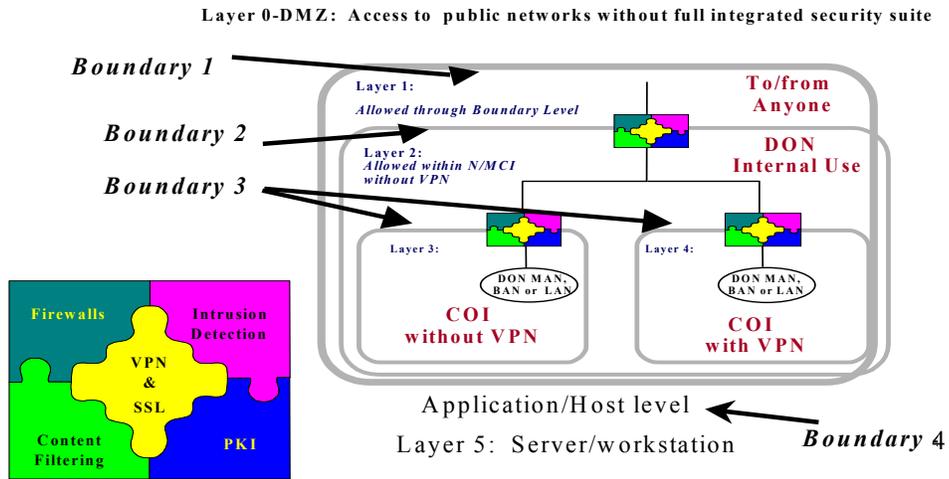
- Flooding system with bogus traffic
- Modification of data in transit
- Spoofing & rerouting attacks
- Compromising networking devices to deny service (penetration of control channels, flaw in product security, configuration errors, hostile modification given physical access)
- Jamming of RF links

Cyber Combined-Arms Attack

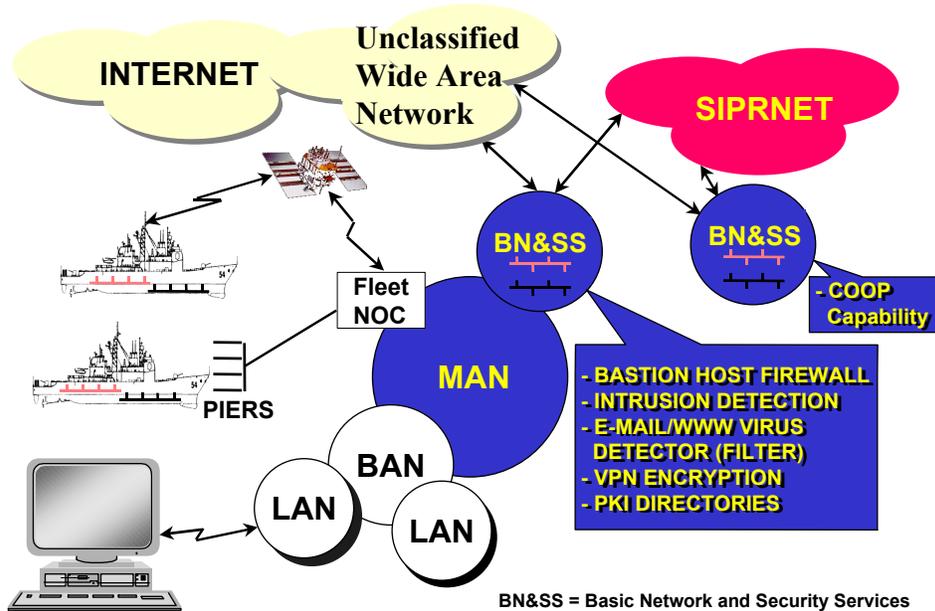
Discovered Latent Vulnerabilities (IAVA, CERT, or Other Reporting Mechanism)  
Heightened INFOCON Status

Appendix 3: Notional N/MCI Security Concepts

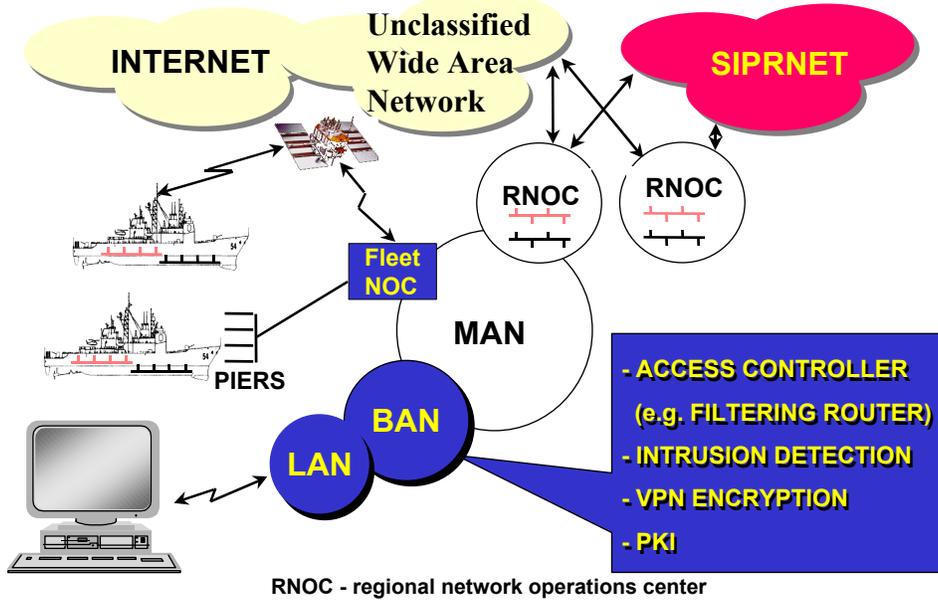
## N/MCI Notional Security Layer Architecture



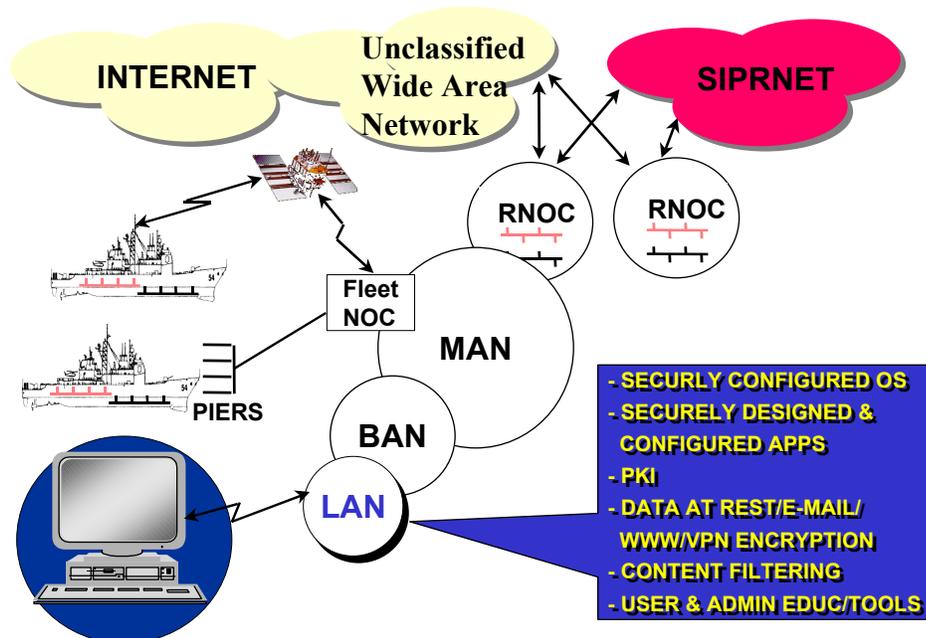
## Defense in Depth: Regional/MAN Level



## Defense in Depth: BAN/LAN or Community of Interest Boundaries



## Defense in Depth: Host Systems



## Naval Firewalls and Content Filtering: Standard Configurations of COTS Products

---

- **Naval Firewall Security System: Standard Configuration**
  - All of the Following
    - Filtering Routers
    - Bastion Host Proxy Firewall (Application Layer)
    - Email virus detector
    - Intrusion Detection System (IDS)
    - Split DNS
    - Web Cache
  - Fleet/MCEN firewall policies are the basis for configuration at Naval sites
- **Network Intrusion Filter (NIF) : Site Specific**
  - One of the Following
    - Packet filtering Router
    - Stateful Monitoring Firewall
    - Bastion Host Proxy Firewall
  - Email virus detector
  - Perhaps a Small Intrusion Detection System
- **Virus Detection & Content Filtering**
  - Systems at firewalls and on individual hosts used
  - Text and attachments
  - Active Content That Executes Locally: Active X, Java, Java Script, VB Script, etc.

## Naval VPN Standards: COTS Criteria

---

### External Considerations

- Navy, Marine Corps and DOD Policies or Guidance
- Commercial Standards
- System Integration Issues
- External Certifications
- Interoperability
  - Between DoN Devices
  - Between DOD Services
- Company Evaluation

### VPN Device Security Architecture

Encryption Algorithms & Protocols

Security Management Features & Protocols

Authentication Algorithms & Protocols

Plaintext Processing  
(filtering, compression, etc.)

Key Generation & Exchange Procedures

Required Network Protocols

Key Protection & Storage

Network Interfaces  
(physical & logical)

- **Many factors should be considered in VPN product selection.**
- **The decisions should be made periodically for DoN as a whole**
  - Maximize interoperability and simplify regional security management
  - Minimize costs: Procurement, training, logistic support, and diversity at BNSS sites.
- **Products from only 2-4 VPN vendors should be deployed in Naval regional and base level security architectures at any given time**
- **Leverage current ANX / ICISA efforts & success in the commercial market**

## IPsec Compliant COTS VPNs: Some Detailed Criteria (Part 1)

---

- **DoN and DOD Policies or Guidance**
  - NSA approved high grade (Type 1) cryptographic products for protection of classified data
  - DOD Policy: No special purpose PKI's.....employ the DOD PKI
  - FIPS 140 certified products (when available) for USG sensitive but unclassified applications
  - DON CIO IT Standards and Guidance:
    - Preference for COTS standards based products
    - IPSEC recommended
- **VPN Device Security Architecture**
  - Encryption Algorithms and Modes:
    - Triple DES or comparable NSA/NIST approved algorithms (key length 80 bits or more)
      - The Advanced Encryption Standard (AES) when available
    - Support for Tunnel and Transport encryption modes
      - Tunnel mode required in some applications
  - Authentication Algorithms:
    - X.509 v3 certificate based authentication (1024 bit modulus size)
    - Support for DOD PKI is critical for scalability
    - Several VPN vendors have already committed to support DOD PKI in their product lines
  - Key Exchange Algorithms and protocols:
    - Internet Key Exchange protocol (IKE)
    - 1024-bit prime modulus Diffie Hellman specified in IPsec standard (Group 2)

## IPsec Compliant COTS VPNs: Some Detailed Criteria (Part 2)

---

- **VPN Security Management**
  - Device security management currently NOT covered by any commercial standards
  - Significant variation in vendor concepts and implementations
  - Community of Interest Separation: Group Support
    - Does product assume one COI and that CA is unique to COI?
      - If so, product is not compatible with use of DOD PKI
      - All Certificate Authorities subordinate to NSA/DISA (not under Navy control)
    - How are group memberships defined and enforced?
      - PKI signed objects? Protected database?
    - Separation of ID certificate from group membership
      - Enables use of DOD ID certificates for client authentication
  - Cross Trust Relationships Between Security Managers?
    - Each VPN device managed by only one security manager
    - Connections allowed between devices controlled by different managers?
      - Allows REGIONAL control of all REGIONAL VPN devices
      - Otherwise cross connections managed by one entity
    - Simplifies joint service and coalition applications
  - Can Software Clients be Managed?

## Detection Mechanisms Built into BN&SS Security Architecture

---

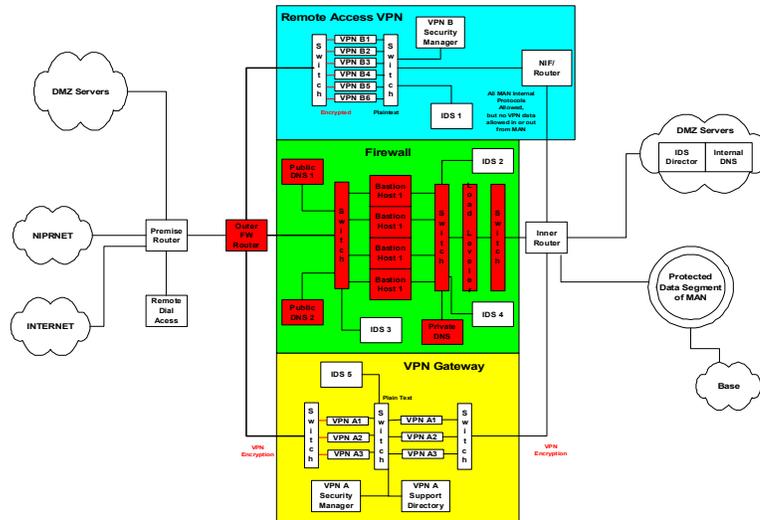
- **Philosophy: The Regional Boundary Does Not Fully Trust Any User**
- **Network based Intrusion Detection Systems**
  - All routes into and out of the BN&SS site are covered
  - Even encrypted data is decrypted and scanned (unless an exception is authorized) before being re-encrypted for transmission over the WAN or MAN.
- **Host Based Intrusion Detection Systems for Critical Servers at BN&SS**
- **Virus scanning applied to all routes into and out of region**
  - Except for VPN gateway used by communities of interest
  - Use of web cache and mail relay is mandatory
- **Content filtering applied to all routes into and out of region**
  - Enforced by bastion hosts firewalls, stateful monitoring firewalls, NIFs, routers, and filtering switches.

## Isolation Mechanisms Built into BN&SS Security Architecture

---

- **VPN SecurityManagement**
  - The VPN security management console can be used to quickly deny access to users who are detected launching attacks
    - The VPN remote access manager can be used to deny external access to or sever cross connections with other sites
    - The VPN gateway manager can be used to deny access
- **Firewalls and NIFs can be configured to block access paths which are not controllable via the VPN management.**
- **Although many intrusion detection systems have active shunning and response modes, these are not currently being used because of concerns about false positives resulting in denial of service. As the technology matures, these features may become more useful.**
- **If the BN&SS is able to remotely manage defenses at the BAN level, then more granular isolation is possible as well.**

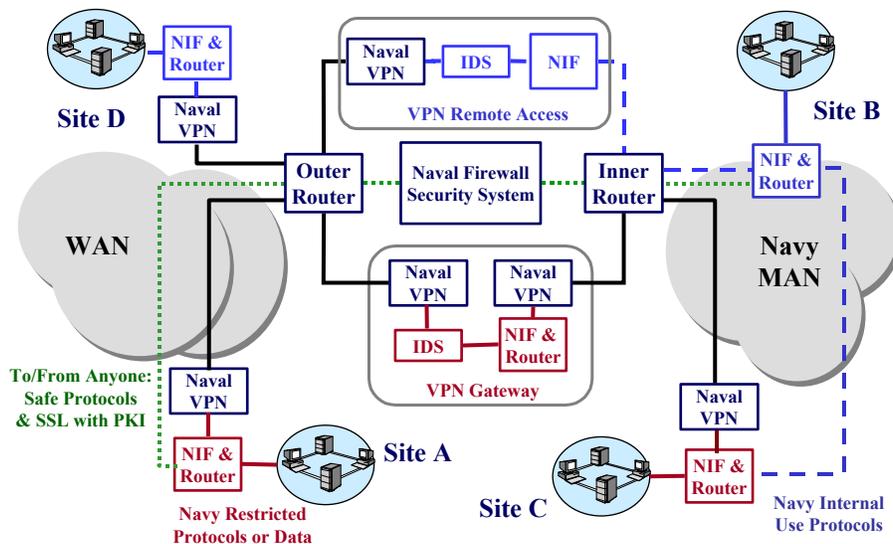
# Notional NIPRNet Security Architecture



## SIPRNET(SECRET IP Routing Network) BN&SS Security Architecture

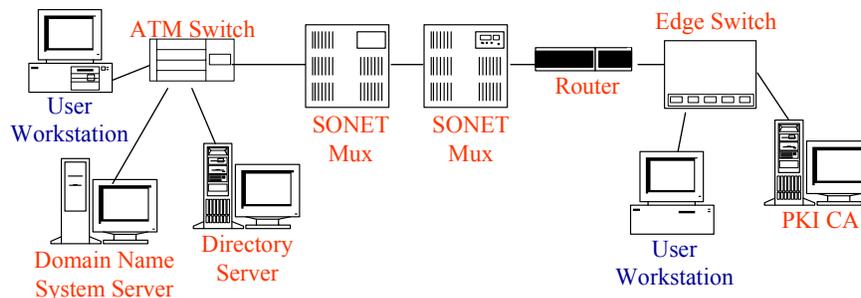
- **The SIPRNET has a parallel boundary defense system (single classification level)**
- **The differences between the Unclassified and SIPRNET are as follows.**
  - **Remote Access:**
    - **Dial up connections to the SIPRNET are via STU-III or STE terminals (high grade devices approved for classified data). So, COTS VPN is required for confidentiality of remote access sessions.**
    - **However, STU-III and STE do not provide specific user authentication. So, a Radius server or VPN device (in authentication only mode) is need to authenticate users.**
  - **VPN Remote Access:**
    - **This path is used primarily to logically connect remote sites on the SIPRNET behind the (SIPRNET) BN&SS security boundary.**
  - **All paths into and out of BN&SS site are encrypted by high grade crypto devices (approved by NSA for classified use)**
- **Once access to the SIPRNET is gained, the security philosophy is the same.**

## The Full Boundary Defense System



## Vulnerabilities of the Infrastructure

- Many types of signaling between and among devices
  - For management, address resolution, routing updates, call setup, etc.
- User-to-switch, switch-to-switch, router-to-router, mux-to-mux, user to DNS, DNS to DNS, user to CA, etc., etc.
- This inter-device signaling rarely authenticated
  - Spoofing can be used for a variety of attacks
- Blocking, redirecting, or slowing the flow of signaling can deny service to the network



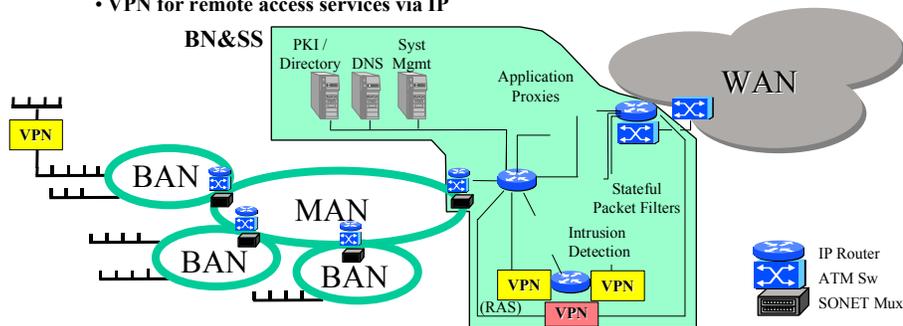
## BN&SS: Additional Security Critical Infrastructure

### Dedicated Critical Network Infrastructure

- Domain Name Server
- Network Time Service
- Network Management
- DON White Pages

### Infrastructure to Support Applications of DOD PKI

- SSL (including client I&A) for Web, LDAP, etc.
- SMIME & DMS messaging
- VPN for remote access services via IP



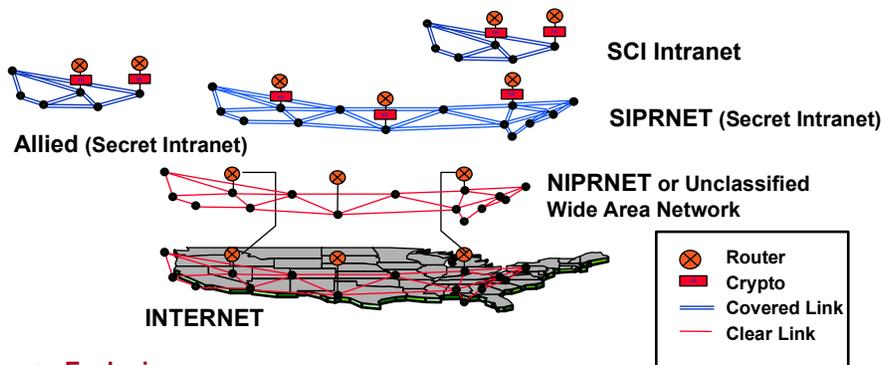
## Components of Defense-In-Depth for the Network Infrastructure (part 1)

- **Authentication of routing protocol updates**
- **Strong, non-spoofable access control for network management**
  - Routers, servers, switches, etc.
- **Protections for vulnerable switch signaling**
  - Not much yet available, so...
  - Networks must be carefully architected
    - Limit the kind of signaling that can pass across N/MCI
    - Provide private or virtual private (e.g. VPN encrypted) connections between elements of the N/MCI to allow flow of signaling information

## Components of Defense-In-Depth for the Network Infrastructure (part 2)

- **Hardened Domain Name System**
  - Pseudo-root forwarders
  - Evolve to cryptographic authentication (e.g. DNSSec) via the current (DoD sponsored) implementation within the Internet
- **Protections for backplane compute services**
  - Similar to protections for customer systems and information
  - Includes Firewalls, network intrusion filters (NIFs), intrusion detection systems (IDSs), securely configured OS, etc.
- **Tools for administrators to continuously monitor security posture**
  - Vulnerability assessment systems (VAS)
- **For classified networks, strong cryptography**
  - Link level and inline network encryptors (INEs) as appropriate

## N/MCI Defense in Depth Strategy: Multiple Security Levels (MSLs)



- ◆ **Exclusion:**  
NSA Approved High Grade Crypto to Separate Classification Levels
- ◆ **Containment:**  
COTS Security Products within Level to Minimize Damage if Penetrated
- ◆ **Risk Management:**  
Balance Containment Against Fiscal Reality