Table of Contents

EXECUTIVE SUMMARY

PURPOSE OF STUDY

Recognizing the information technology explosion of the Information Age and its impact on the Department of the Navy (DON), the Assistant Secretary of the Navy for Research, Development and Acquisition asked the Naval Research Advisory Committee (NRAC) to convene a panel to study Naval Information Warfare Defense. The Panel focused its attention on vulnerabilities and threats, technology, policy, operations, training and acquisition. It assessed the DON's increasing dependence on information to carry out its mission, identified Information Warfare - Defense (IW-D) shortfalls, reviewed areas requiring increased attention and investigated technologies which should yield significant enhancements if Naval services were to invest in them. The Panel feels that this report can serve as the basis for an affordable DON IW-D roadmap.

STUDY APPROACH

The esoteric nature of the topic required significant background knowledge. Accordingly, subject matter experts were invited to join the Panel. Briefings, demonstrations, and fleet tours focused on the DON's Information Warfare protection and attack detection process. Guided by a risk management approach, emphasis was placed on identifying steps to improve and assure the effective performance of the DON's information networks in the face of adversarial efforts to disrupt or degrade U.S. Naval operations.

KEY POINTS

During the course of this study, the Panel identified several critical key points that relate to their conclusion:

- Naval forces are absolutely dependent on information, including quality and integrity.
- Information systems are increasingly vulnerable to IW attack, particularly with increasing networks, connectivity and operating nodes, including use of commercially available satellite communications (SATCOM).
- Information Warfare (IW) threats do exist; they range from random incidental corruption to focused attempts to deny, degrade, deceive, destroy, or exploit as a military advantage.
- Risk managed IW-D is possible; issues and solutions need to be prioritized on the basis of technical, operational, and economic readiness.

- Action should be started now, with attention to both near-term, prioritized, protective measures and long-term process improvements, including promulgation of strategy, policy, and training.

TECHNOLOGY ASSESSMENT

The flood of information expands well beyond military-critical needs to include administrative and human resource needs and independent personal use of the Internet, bringing about a significant reliance on (or at least use of) commercial and military SATCOM, whether driven by bandwidth needs or economic desires.

The impact is that several domains can become commingled, each at a different security level but with common links which, in turn, can lead to a common network that provides unauthorized access and potential entry points from transmission through storage. In addition, introduction of commercial SATCOM raises a serious concern; namely, the fleet's vulnerability to being located.

Initial network protection success can be attained through operating discipline; i.e., network administration and security management, access control rules and audits, and identification and authentication procedures for users.

Those technologies which the Panel believes critical for network protection are: 1) Firewalls and Guards to enhance domain compartmentalization and provide controlled transfers between domains; 2) Monitoring and Probing tools to facilitate network administration, management, real-time monitoring, and reactive capability; and 3) Embedded Encryption to protect bulk files, support domain level file and digital signature identification and authentication.

There is considerable concern about the use of commercial satellites, with their significant vulnerabilities and limited built-in security. The Panel does recognize the economic benefits associated with their use, and encourages technology efforts to mitigate the relative ease of jamming inside the subscriber footprint, together with power management operational procedures and gateway modifications compatible with emission control (EMCON) conditions to minimize geolocation.

RECOMMENDATIONS

After a lengthy discussion of the specific topics and issues noted in detail in the body of this report, the Panel believes that improved IW-D capabilities are mission-essential and that IW-D needs to be raised as a DON priority.

Accordingly, the Panel offers the following five Summary Recommendations:

1) **Establish a DON-wide network protection effort** which integrates best security practices into standard operating procedures, increases IW-D research and development (R&D) investment for the critical areas noted above, and embraces the Acquisition Systems Protection Program to provide information assurance in key Naval systems.

2) **Train and educate Naval personnel** to build IW-D expertise and promote user discipline.

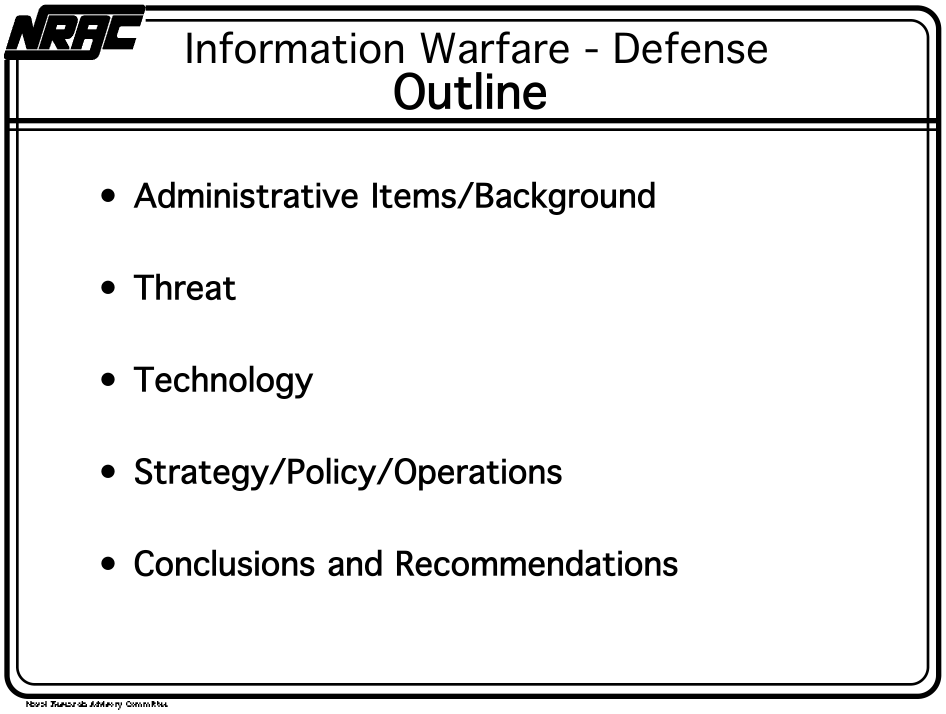
3) **Mandate aggressive implementation of IW-D in all Naval exercises** to explore vulnerabilities and to generate doctrine, requirements, tactics, techniques and procedures.

4) **Accelerate promulgation of a DON IW-D strategy and policy** by appointing a Chief Information Officer (CIO) as the Naval focal point, designating warfare responsibility for operational IW-D and establishing a formal legal framework for policy development and execution.

5) **Engage in the Department of Defense (DoD) and national debate** to enable the DON to capitalize upon a unique opportunity to ensure that Naval force missions and needs are adequately considered.

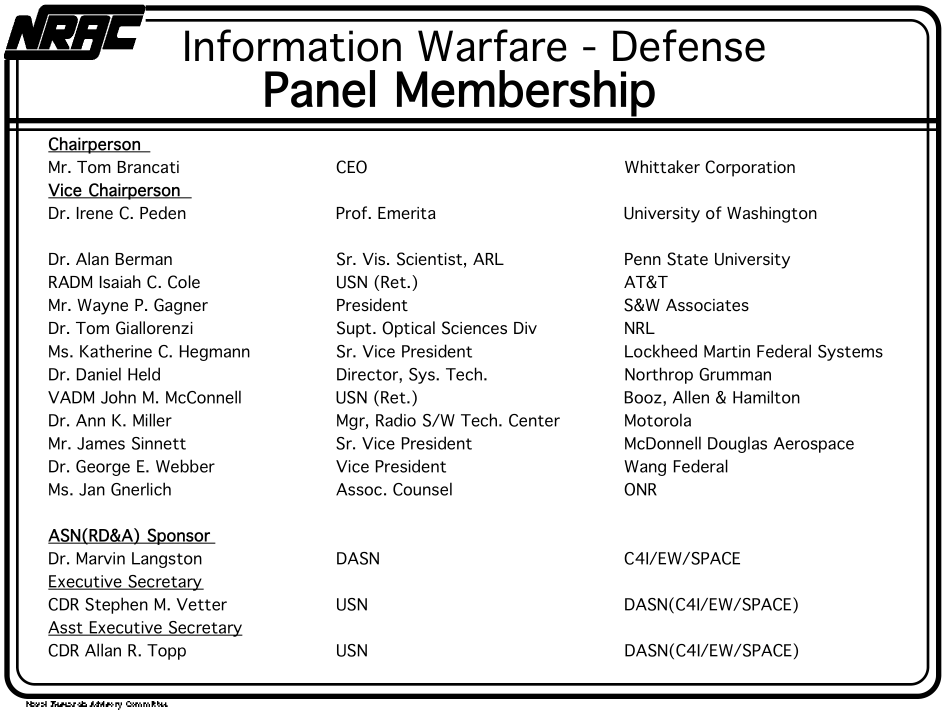
Additional specific recommendations are included in the text for capability, strategy and policy, management, and expertise issues.

The Panel feels strongly that acting now to address the issues raised herein will enable the DON to attain an acceptable level of security at what appears to be a reasonable cost.



OUTLINE

The NRAC IW-D Report is organized into five basic areas. Following an initial statement of the study tasking, participants and sources of information, the Report addresses characterization of the information threats, technology issues and needs, and strategic and policy issues, which lead to a set of summary recommendations based upon the Panel's findings in each area.

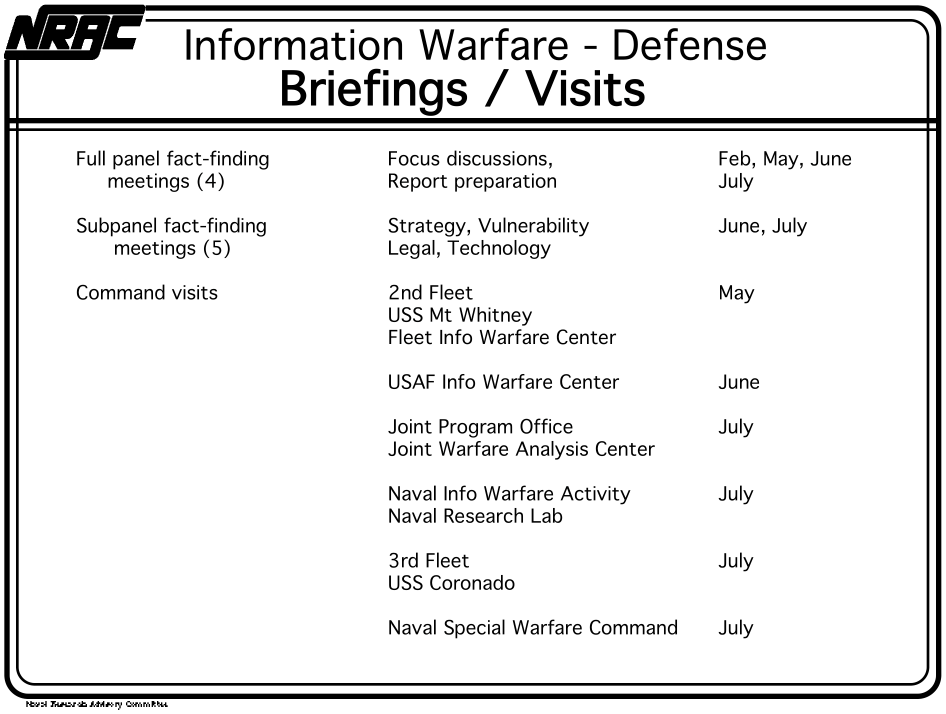


PANEL MEMBERSHIP

The NRAC IW-D Summer Study Panel was composed of representatives from industry, academia, and the Navy science, technology, and legal communities. Six NRAC members were complemented with a cadre of experts with diverse talents to address this issue.

The sponsor of the study was Dr. Marvin Langston, Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers and Intelligence, Electronic Warfare and Space programs [DASN(C^4I/EW/SPACE)].

The study topic was proposed in the fourth quarter of 1995 and the NRAC Panel began its deliberations in February 1996.

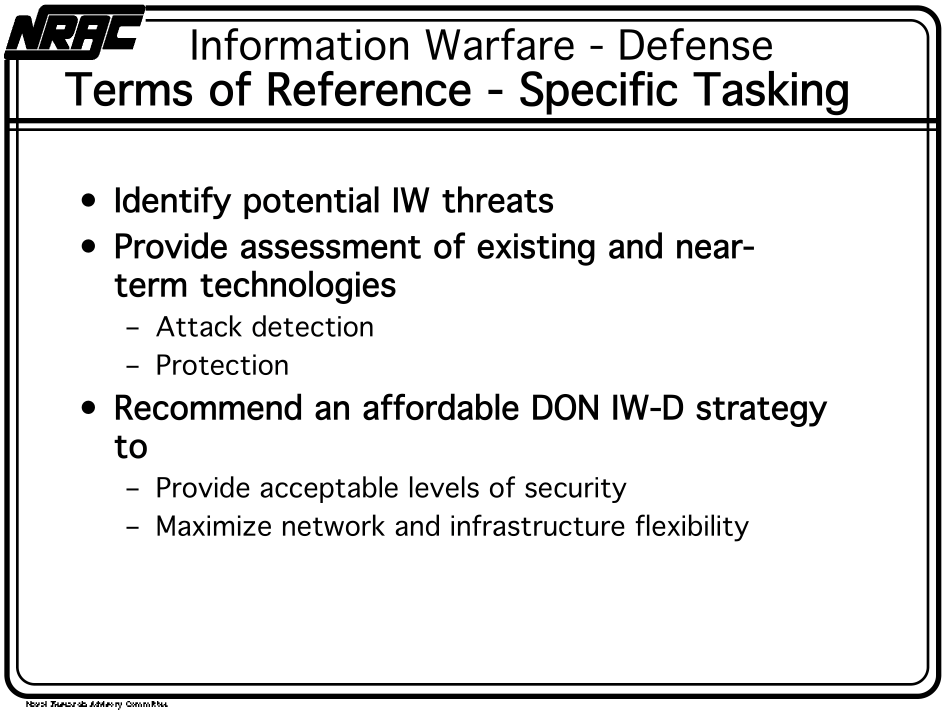


BRIEFINGS / VISITS

A number of panel meetings and visits were conducted prior to the final two-week report preparation period. Discussions and planning meetings were interspersed between command visits to the 2nd and 3rd Fleet Command Ships, U.S. Air Force, Navy, and Fleet Information Warfare Centers, and to the Joint Program Office, Joint Warfare Analysis Center, Naval Research Laboratory and Naval Special Warfare Command. The Panel was divided into three Sub-Panels to provide specific focus on vulnerability, technology, and legal/strategic/expertise issues.

The Panel gained a solid understanding of existing fleet capabilities and plans for increased capacity as supported by technology growth, including commercial communications outside the fleet as well as those within the military infrastructure. The Panel found a strong consensus at the operating level for the need to protect operating networks, to defend against SATCOM vulnerabilities, and to generally elevate the level of the IW-D effort within the DON.

In the final days of deliberation, the Panel concentrated on identifying those elements which are essential for generating immediate benefits, and on outlining a long-term process improvement strategy.



TERMS OF REFERENCE - SPECIFIC TASKING

In February 1996, NRAC was charged with an assessment of the DON IW protection and attack detection processes. The general objective called for a technology assessment to enhance the development and protection of emerging Naval networks from first order vulnerabilities.

For the purpose of this study, the Panel focused on threats (susceptibilities and vulnerabilities), technology elements, and the emerging DON policy to mitigate both near- and long-term risks.

The specific Terms of Reference for the NRAC Summer Study Panel on IW-D are included here in their entirety.

Terms of Reference

Assessing DON Information Warfare

Protection and Attack Detection Processes

GENERAL OBJECTIVE: Assess technologies associated with the protection and attack detection processes in order to enhance the development and protection of emerging Naval networks from first order vulnerabilities.

BACKGROUND: The DON is in the process of interconnecting a substantial portion of its operational and support infrastructure (voice, video and data) in order to enhance productivity across a variety of disciplines, including Automated Information Systems (AIS), Medical, Personnel, Acquisition, Operations, Intelligence, etc. This network will include fiber, wire, satellite and wireless, including line of sight radio frequency (LOS RF), elements.

Guided by a risk management approach, particular emphasis should be placed on identifying steps to be taken now so as to assure the effective performance of DON networks (fiber, wire and RF) in the face of likely adversarial efforts to disrupt or degrade their support of U.S. Naval operations. The specific focus will be on recommending a strategy to include such things as identifying and prioritizing policy, technology and/or program developments for incorporation into Naval networks and support infrastructures.

SPECIFIC TASKING:

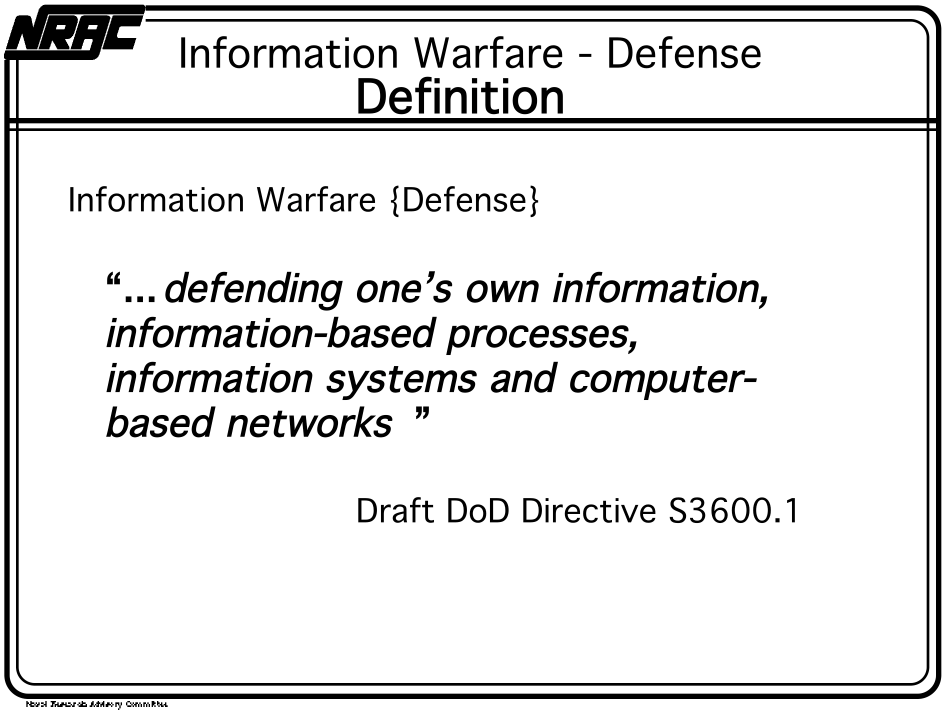
a. Identify potential IW threats.

b. Provide an assessment of existing and near-term attack detection and protection technologies.

c. Recommend a DON defensive IW strategy that provides acceptable levels of security while maximizing network and infrastructure flexibility at an acceptable cost.

ASN(RD&A) Sponsor: Dr. Marvin Langston, Deputy Assistant Secretary of the Navy (C^4I/EW/SPACE), (703) 695-0023

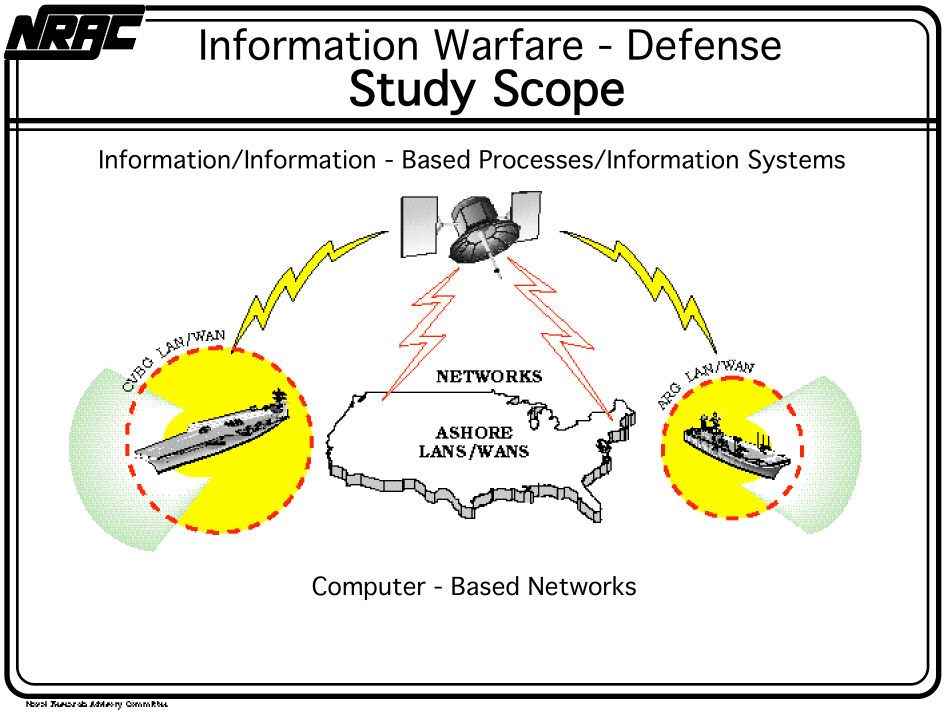
POINT OF CONTACT: CDR Steve Vetter, Office of the Deputy Assistant Secretary of the Navy (C^4I/EW/SPACE), (703) 602-7930



DEFINITION

The Panel discovered that there are so many issues and elements of IW (networks, data storage, retrieval, and transmission via satellite networks) and differing perspectives that any true definition is probably in the eyes of the beholder.

However, for the purposes of this study, the Panel chose that definition which appears currently in draft DoD Directive S3600.1 and previously in DoD Directive TS3600.1. In the context of IW-D, this may be stated as, "...defending one's own information, information-based processes, information systems, and computer-based networks."

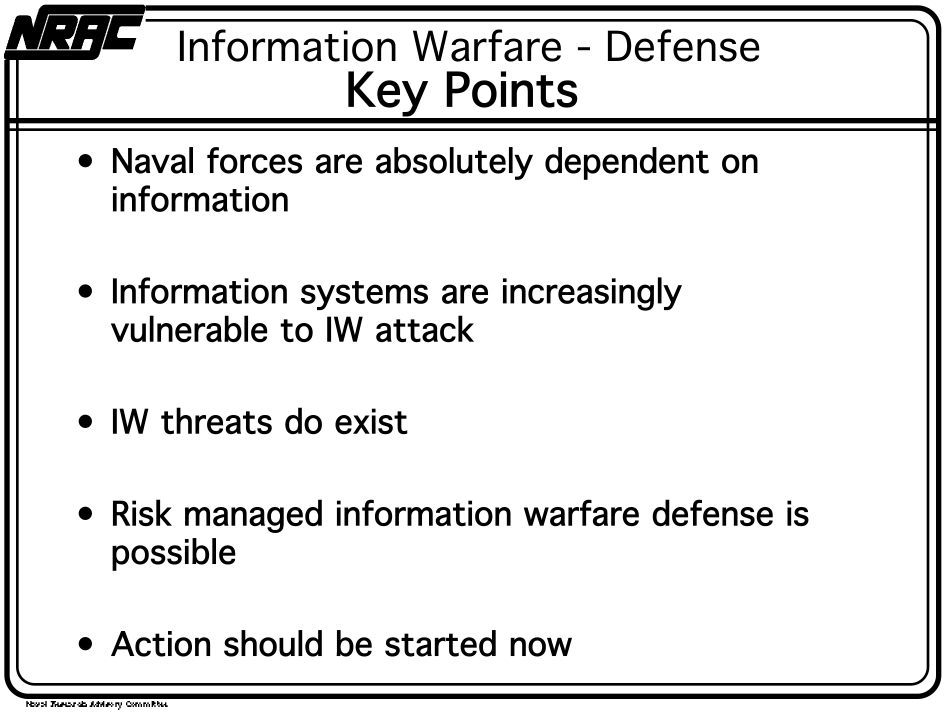


STUDY SCOPE

Information, information-based processes, information systems, and computer networks encompass the realm of information flow or communication within and between battle groups and between ships and shore. Local and wide area networks (LAN and WAN), both ashore and afloat, have become increasingly more reliant upon satellite networks to provide linkage as both the magnitude and rate of information traffic escalates.

To the extent that it was affordable, reliable, secure transmission of information was included in the design requirements of military communication satellite systems. However, similar protection measures were not incorporated in the design of commercial SATCOM systems.

These commercial systems provide cost effective means for information transfer. Commercial off-the-shelf (COTS) acquisition initiatives will increase reliance on these systems. Thus, the scope of the Navy's IW-D concerns must include the combination of military and commercial systems which comprise the global Naval communication and information network.



KEY POINTS

Forward deployed Naval forces are increasingly dependent upon the availability, quality and integrity of massive amounts of information in order to carry out their mission. The coordination of fleet operations has become progressively more dependent upon connectivity ashore and afloat for real-time situation awareness. Additionally, the forward-deployed fleet relies on rapid turnaround of non-critical information for administrative support, logistics and improved quality of life.

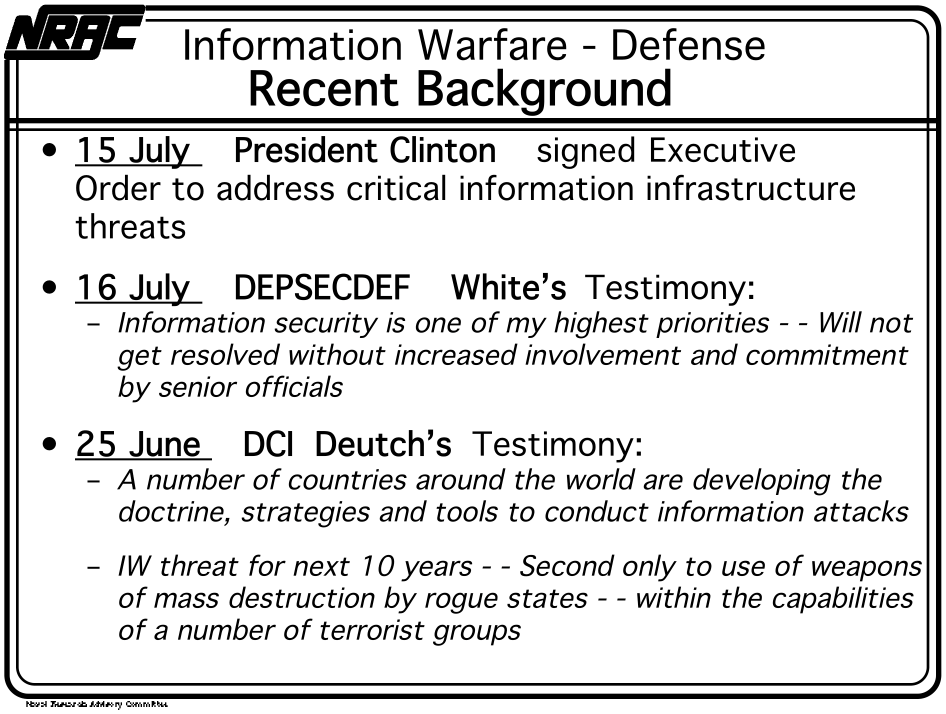
These information needs, coupled with the lack of an evident threat, has led to the proliferation of a widely diverse set of networks and a concomitant laxity in security enforcement. These information systems are increasingly vulnerable because they can be penetrated through the networks by which they are connected. Such acts may range in seriousness from an accidental disruption or corruption of data to deliberate exploitation or denial. It is clear that IW threats do exist; but, the ability to defend against them has not grown proportionately and the Panel found no formal process to convert susceptibilities into IW-D requirements.

A detailed vulnerability analysis that includes examining the individual nodes and the network entry points, can be used as a first step to rank order the individual risks to network and system security. A set of

priorities may be established beginning with the most critical risks and usage points to provide a layered defense against IW.

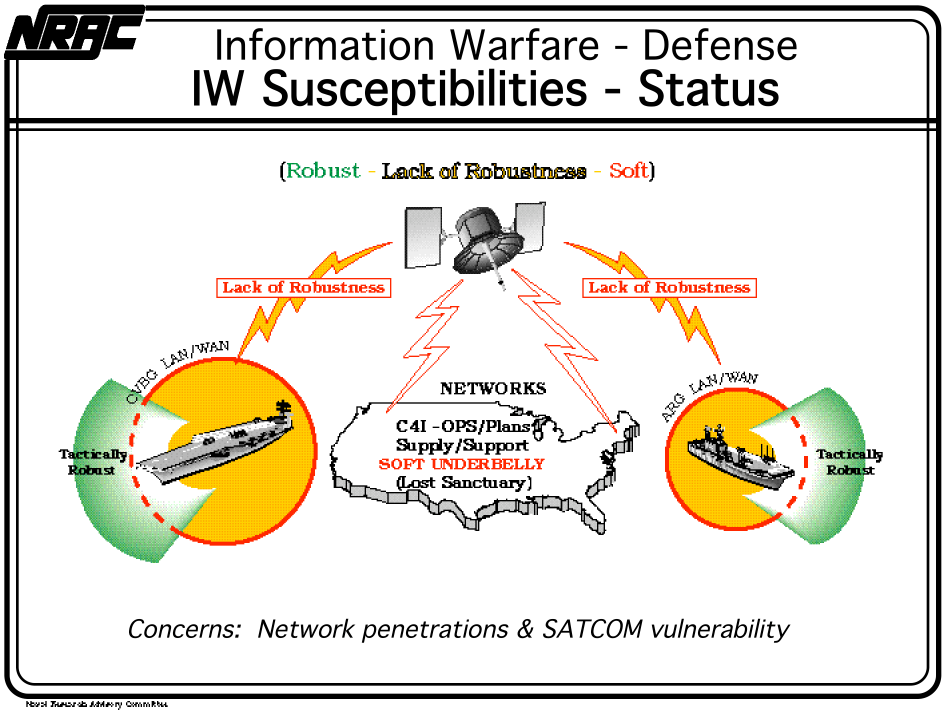
Certain actions should be started immediately to identify and secure those areas which can be secured with minimum investment, or which may have far-reaching impact if compromised. Specific steps are recommended later in this report. The Panel felt that the cycle-time for requirements definition and development of adequate safeguards and countermeasures needs to be collapsed to be within the time scale of emerging information technology and systems development.

In addition, the Panel felt that there is an urgency to promulgate an IW-D strategy and policy and to elevate the priority of IW-D significantly.



RECENT BACKGROUND

The existence of an IW threat has been readily accepted by senior members of the U.S. Government. President Clinton has signed an executive order to address the critical information infrastructure threats. This position is supported by Director of Central Intelligence (DCI) John Deutch's testimony to Congress that emphasizes that INFORMATION WARFARE is second only to the threat of weapons of mass destruction by rogue states. He noted that the ability to launch an IW attack is also likely to be within the capabilities of a number of terrorist groups "which themselves have increasingly used the Internet and other modern means for their own communications." Deputy Secretary of Defense (DEPSECDEF) White has testified that information security is one of his highest priorities and that resolution can only be accomplished by increased involvement and commitment by senior officials.



IW SUSCEPTIBILITIES - STATUS

Naval systems have been developed to respond to fleet requirements. In the past, carrier battle groups (CVBG) and the Amphibious Ready Group (ARG) operated in a robust information security mode with organic fleet systems that were complete, operational, and the principal sources of information. Fleet LAN/WAN systems operating in a battle group environment successfully handled the daily information traffic and command decisions for all ship, amphibious, and air operations. This relatively closed operational status allowed operations in ocean areas long distances from foreign and domestic intrusion and interference potentials.

The introduction of commercial satellite communications and other information configurations, both shorebased and afloat, while permitting the handling and transfer of a significantly increased volume of information, has allowed vulnerabilities to creep in. The ability to attack communications links and unclassified systems for logistics, personnel, medical, finance, and transportation creates a situation with a lack of robustness. The security of current commercial SATCOM services and networks is easily compromised; this includes the capability to geolocate fleet users.

The operational capabilities of Naval forces are strengthened with each new network and data system that supports and enhances weapon

targeting and C^4I operations. Each Naval operation is supported by information automation. Networking is required for efficient and rapid transfer of data from organic and remote providers.

The proliferation of Naval networks allows interoperability of data, but data networks allow more opportunity and points of vulnerability for intrusion and exploitation. The ease of exploitation and the availability of concepts to intrude into networks are rapidly growing.

The proliferation of networks ashore and afloat and the interconnection of these networks provides mission-essential information to Naval forces. However, this architecture lends itself to possible penetration by an adversary from great distances. This means that we have lost our information sanctuaries both ashore and afloat.

SATCOM DEPENDENCY IS REAL

The throughput of communications from the SATCOM system to the command ship is projected to increase sharply in the next decade. The rate of information transfer measured in megabits per second (MBPS) will continue to grow and to tax the capacity of projected military SATCOM systems.

The projected increase in both simplex and duplex service requirements will lead to the use of bought or leased commercial SATCOM services to handle as much as 85% of the total simplex requirements.

The sharp increases in demand that started in the mid-1990s will continue to grow with the use of current and planned systems. Traditional services, such as intelligence and command and control, provided by SATCOM to the fleet will be augmented by new services such as medical, reconnaissance, financial, surveillance, logistics, targeting, meteorological and oceanographic information (METOC), morale, welfare and recreation (MWR), and situation awareness. Each support function for a command ship will require growing data rates as systems are upgraded and enhanced. Joint military operations in the future will require larger interactive distributed networks for fleet requirements. The Gulf War demonstrated a number of similar growth requirements needed for joint operations.

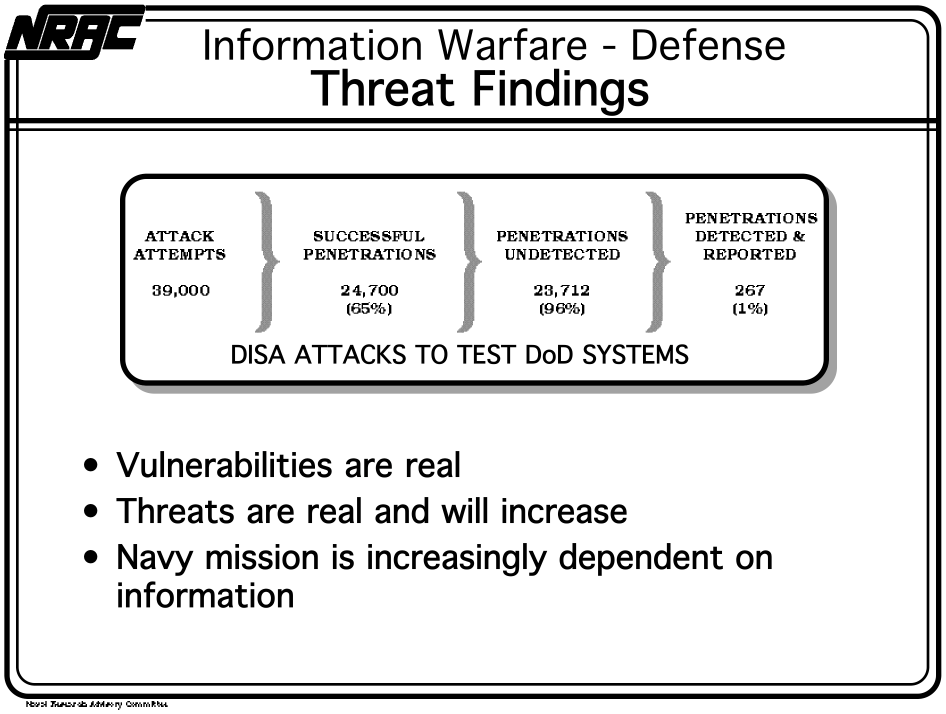
In the recent past, design of Naval Communication systems was dependent upon the requirements for relaying intelligence C^2, and targeting information.

Currently, additional fleet utilization and the requirement to handle larger volumes of information, processed at higher speeds, and provided to the user in real time, have significantly increased demands on our communications satellites.

SATCOM usage will increase with system and sub-system demand from emerging Naval networks and will continually press the Naval communications network for additional SATCOM capacity.

The MILSTAR system (MDR III) is projected to be on-line by the end of 1998. This duplex capability offers an enhanced military system with an acceptable level of anti-jamming technology and denial of service protection.

Commercial systems will continue to provide high bandwidth simplex services for the foreseeable future through lease and buy arrangements. Many of the non-critical fleet demands will be provided by commercial systems. Our concern is that military usage of commercial systems is susceptible to jamming, other forms of denial of service attack, exploitation and geolocation; hence they require plans for alternate operations, particularly during EMCON.



THREAT FINDINGS

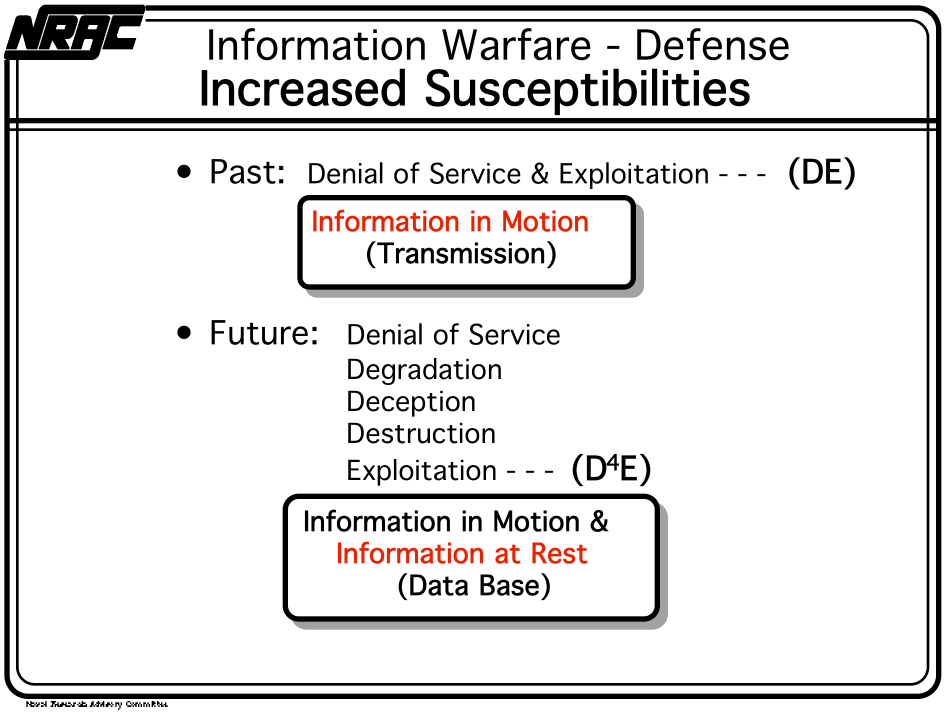
Vulnerabilities of Naval systems are real and tend to increase with the introduction of new equipment in the international market, the proliferation of additional software and intrusion techniques, and the growth of adversary groups throughout the world. The DON's enhanced usage of emerging and interconnected networks creates additional points for intrusion and an increased number of vulnerable connection and interface points. Threats developed by the former Soviet states, commercial components manufactured throughout the world, equipment from hostile actions involving other countries, and an increased awareness of intrusion techniques constitute a set of susceptibilities that are affordable and available to any adversary.

The standards of information system design, performance, and architecture all have their origins in the U.S. These standards provide a common baseline for all countries to acquire and utilize equipment for peaceful and adversarial roles. The lower costs and greater availability will lead to increased use by individuals, dedicated groups, and rogue states.

All DON C^4I, weapons and support systems utilize networks that pass, record and store data for Naval operations. Deception and degradation of data can be subtle and difficult to detect. Degradation or loss of a system lowers operational efficiency and decreases the ability to

perform required functions. The end user's requirement to use a minimum amount of weapons with the highest degree of accuracy and lethality demands a data flow that is accurate, timely, of high quality, and assured integrity. There is no room for data of unknown origin, low quality, and unverified integrity, given the increasing dependence of the DON's mission on accurate and immediate information.

A report by the General Accounting Office (GAO) notes Defense Information Systems Agency (DISA) findings that verify that test attacks designed to penetrate DoD systems have been generally successful and mostly undetected. Undetected penetrations ran as high as 96% of the 39,000 test attacks.



INCREASED SUSCEPTIBILITIES

IW susceptibility is changing with the increased usage of systems in Naval operations. Historically, information security concentrated on the transmission of data, i.e. "information in motion." Information in motion continues to increase and is subject to denial of service and exploitation. In the past, data formats were hard copy in most cases and were not electronically stored. Physical security measures could adequately protect the data in storage, "information at rest." Prior operations provided considerable capability to deny intrusion and exploitation. U.S. systems and technology were in the forefront of advancements and our budgets allowed for extensive design and operational protection. The transmission of data was on a limited basis compared to today's interactions with their very high electronic content.

The DON's information systems are rapidly becoming completely based on massive electronic storage of data. The interconnection and the electronic use of data now subject these systems to the possibility of denial of service through degrading, jamming, overload, and insertion of false or misguiding data. The ability to deceive is growing with the ability to penetrate a system and the readily available techniques and tools for deception, destruction, and exploitation of stored data. Naval dependence upon stored data grows exponentially with each application of information technology. The ability to conduct successful military operations in a joint, littoral environment, with quality intelligence and precision strikes,

requires the management and use of these databases, i.e. “information at rest.”

The combination of data at rest in electronic form and data in motion creates increased susceptibility.

There are five basic areas of network susceptibilities:

- Denial
- Deception
- Degradation
- Destruction
- Exploitation

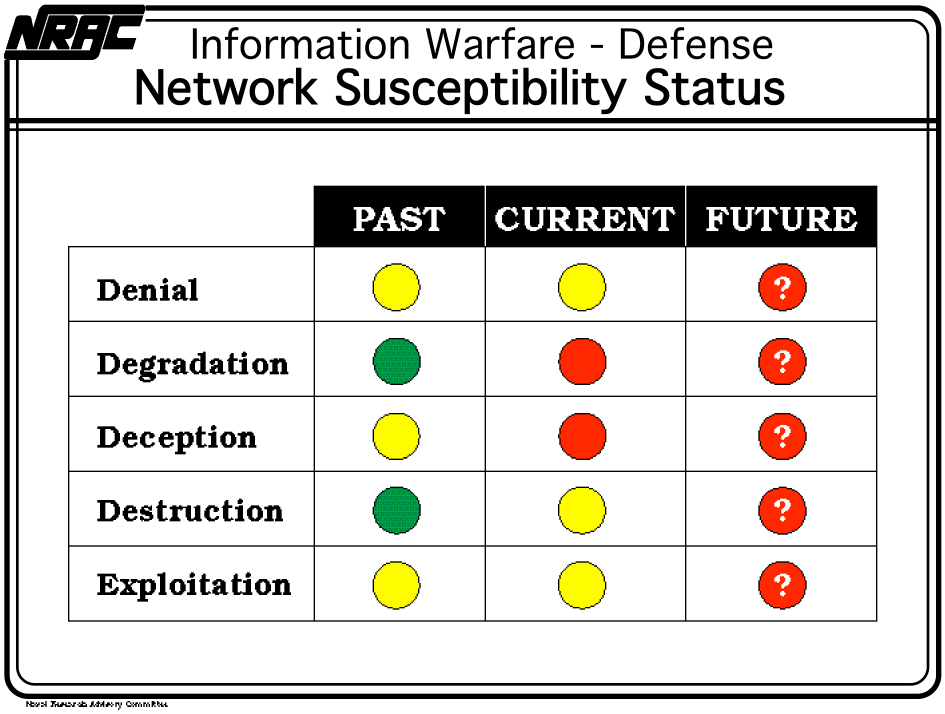
Denial of service includes jamming, front-end attack, and nodal closure. In many geometries, communications jamming could be defeated with an investment in Anti-Jamming (A-J) technology.

Degradation of service is the alteration of data within a network. Past operations relied on hard copy records to store data which were difficult to alter. Current systems use electronic data storage that is growing at a fast rate and is subject to alteration, with limited capabilities to detect or stop attack and intrusion.

Deception includes the alteration of data and actions to alter perception. Past actions involved adversaries capable of inserting “masquerade” data and misrepresenting or intentionally leaking data. Currently, networks cannot determine electronic masquerading. In the future, Naval networks will encounter a proliferation of interfaces and interoperating networks that will create more vulnerabilities.

Destruction in a system results in destruction of data. Past operations required physical attack on the storage facility which was very costly. Most current networks have data files, and these can be penetrated.

Exploitation of communications allows an adversary to determine activity, capability and intent from national through tactical levels. In the past, exploitations were dependent on communications intelligence (COMINT) and signals intelligence (SIGINT) capabilities that were common and effective. SIGINT capabilities have continued to expand and are still operable. The Panel’s concern is that future adversaries will use networks and their interoperability to create points of entry for intrusion.

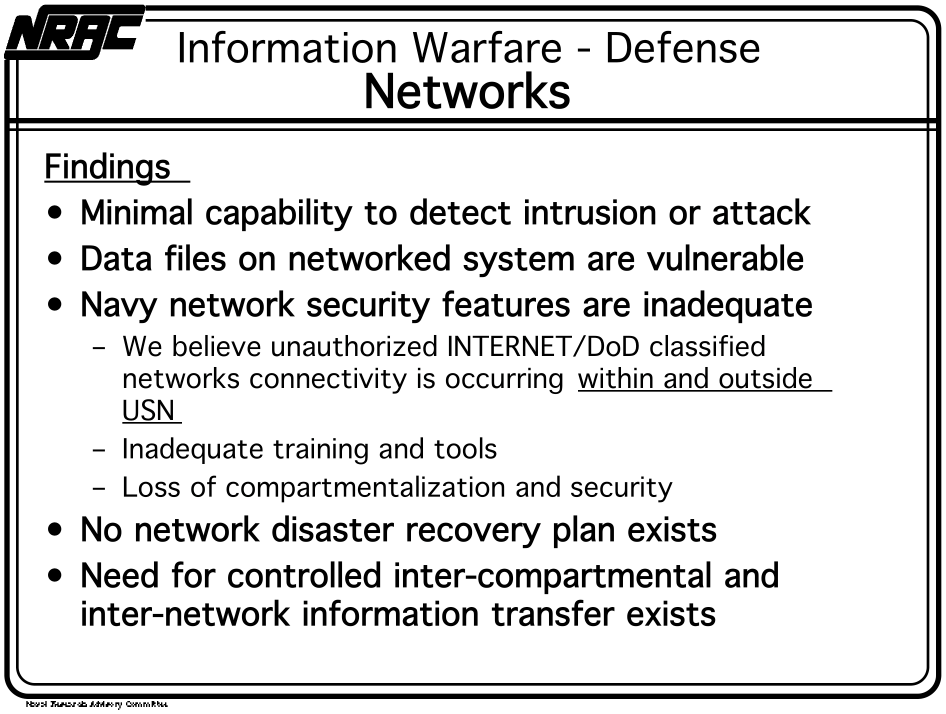


NETWORK SUSCEPTIBILITY STATUS

This stop light chart indicates susceptibilities, both past and current. Denial of service attacks are now and have been in the past a source of concern. If use of and dependence upon commercial SATCOM services increase, the lights may become red in the future. In the past, it was difficult for an enemy to degrade or destroy data held in hard copy form in physical storage. Data at rest could be protected. The situation is not currently red, because the DON has not yet transitioned to totally electronic storage of data.

In the past, an enemy's ability to deceive Naval sensors has been a source of concern. Since networks can now be intruded and databases can be altered, the DON's susceptibility to deception may turn into a red light. The challenge grows with additional networks and interfaces.

If susceptibilities to IW attack cannot be mitigated by IW-D in the future, there is a real potential for all the traffic lights to turn red. Appropriate operational and technology actions must be taken to prevent such an occurrence.

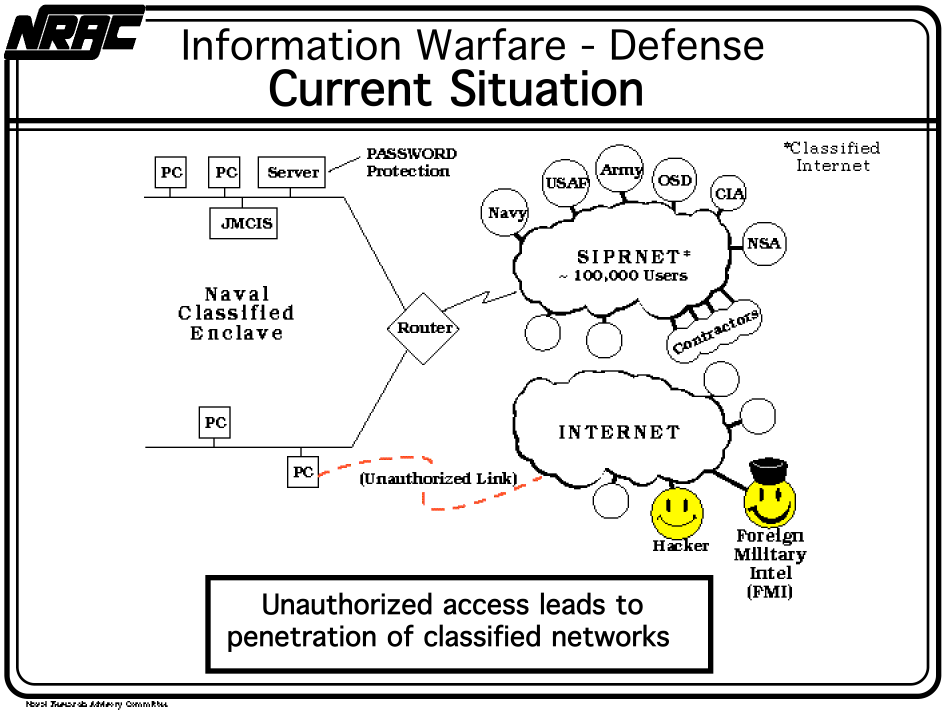


NETWORKS

In reviewing the DON's current use of networking and computer technology in fleet operations, the primary observation is that information technology has been widely deployed and used without a comprehensive integrated strategy for protection of information. The DON's dependence on this technology is growing extremely rapidly to the point where it is now a mandatory element for accomplishing nearly all missions. The lack of a well quantified network threat has resulted in laxity in the development and implementation of a computer and network security strategy. The Panel believes that threat quantification can only be achieved through operational exercises of the entire information system, to include challenges to system integrity at each sub-element (sub-domain) level. Waiting for definitive threat attempts via the intelligence process may preclude timely corrective actions and response, due to the surreptitious nature of the event and detection-identification-correction timelines.

One of the important objectives of this investigation was to attempt to identify and recommend cost-effective emerging "protective" technologies which, although they may not provide perfect protection, will serve to significantly enhance information protection by contrast to current practices, and yet will enable the DON to retain many of the operational advantages of using the latest networking and related information technologies.

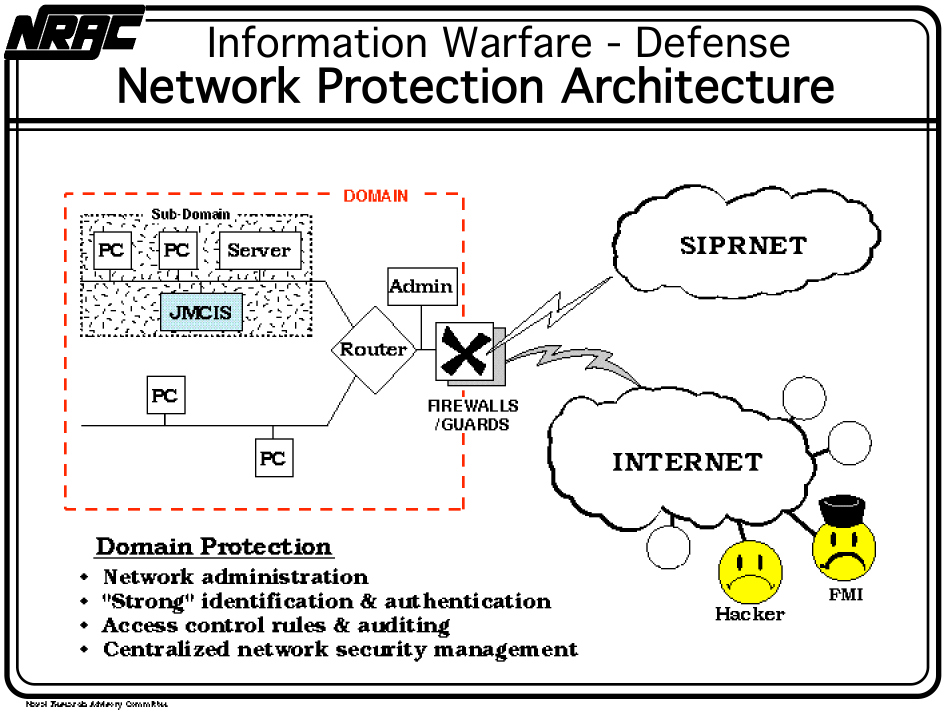
Within the DON and the DoD as well, networking technology has already enabled the interconnection of a tremendous number of information resources. This has primarily involved Sensitive-But-Unclassified (SBU) and Unclassified systems such as DISNET and INTERNET. However, there is evidence that unauthorized and uncontrolled connectivity has also been extended in some situations to include Secret level systems and the SIPRNET network as well. Although the Navy's Copernicus architecture does generally speak to some of the security related issues and technologies involved in addressing these problems, at this time there is not a comprehensive DON-wide protective strategy which is either widely understood or being implemented in order to control and protect the storage, the release, and the transfer of information among authorized users in this complex interconnected environment. From a DON operational viewpoint it is no longer acceptable to simply conclude that, "in the interest of security," no electronic connections will be permitted across security levels through networks except via manual review and transfer. It is a fact today that the timely but controlled transfer of certain authorized information between dispersed systems and even across security boundaries must be facilitated in order to meet tactical as well as strategic operational requirements. As an example, the DON Joint Maritime Command Information System (JMCIS) system must have timely access to authorized intelligence information, as well as to authorized but classified Joint-Service (CINC level) mission plans, and to unclassified support data.



CURRENT SITUATION

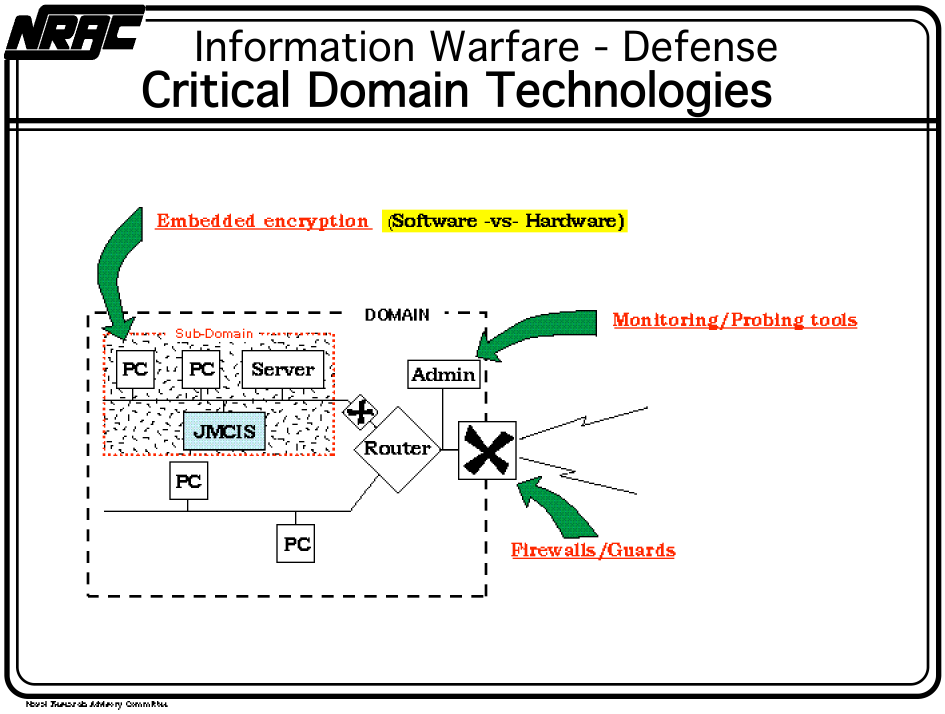
Currently most DON systems which are either knowingly or unknowingly connected to various operational networks provide very little, if any, protection of information or control in the release and transfer of information. For the most part they rely on the old "system high" principles of operation, based on the assumption that any user or system connected to the network is appropriately authorized for any information in the network and therefore can be trusted not to engage in improper exploitation, modification or release of information. As an example of the problems which arise with this kind of assumption, it is worth noting that the current Secret level DoD Internet (SIPRNET) includes over 100,000 approved users and system connections around the world. The only controls currently implemented for managing access to information on the SIPRNET are based upon simple "password" techniques which may or may not be implemented at an individual system level. In most cases, even these techniques are not uniformly used and administered; they have repeatedly been shown to be easily defeated. Separate from the issue of the questionable integrity of 100,000 "authorized" users, numerous incidents have also been reported that involve direct and indirect connections between these classified networks and the unclassified INTERNET. With today's network technology and the large numbers of users and information providers involved, the old concepts of "system high" operations without strong identification and authentication and compartmental protections based upon "need-to-know" rules are simply

too naive to ensure adequate security and integrity of critical information assets.



NETWORK PROTECTION ARCHITECTURE

Based upon these observations, one of the highest immediate payoff areas of investment for IW-D would be in those selected technologies which can provide the capability to define and protect operational "domains" of information within wide area networked environments. This would include technologies related to the strong identification and authentication of users, as well as to file protection of information residing within operational "domains," and to technologies involved in controlling the release and transfer of information between "domains" when required. Also included would be technologies involved in automating network administration functions and network security monitoring and security management functions.

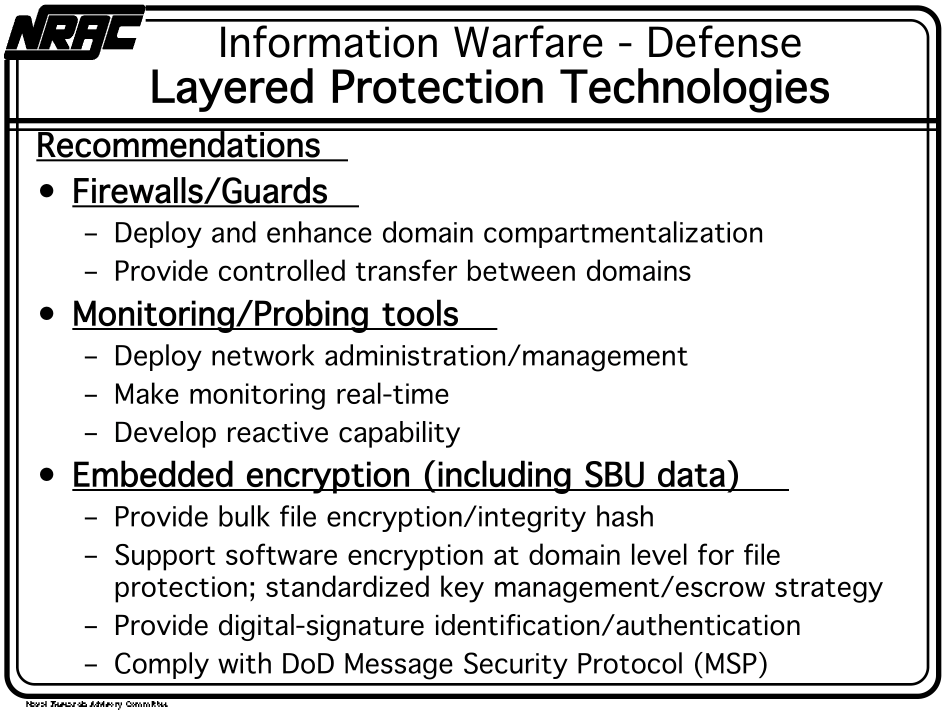


CRITICAL DOMAIN TECHNOLOGIES

The first and most important of the recommended network protection technology investments should focus on the development and deployment of technology capable of providing a DON-wide basis for "strong identification and authentication" of users and processes across networks. Reliable identification and authentication is an absolutely mandatory requirement for implementation of any security control policy in distributed, network-based systems. The best technical approach for achieving a strong identification and authentication capability for the DON is through the use of digital signature techniques using token-based public key encryption (PKE) technology. This kind of technology is currently being developed at the DoD level as part of the MISSI/FORTEZZA program in support of the Defense Message System (DMS). In addition to the identification and authentication capabilities provided by the token-based PKE technology, the DON should also exploit the inherent capabilities of the technology to provide data integrity protection (hashing), data confidentiality, and non-repudiation at the message level. Whether or not the DON elects to standardize upon and use directly the MISSI/FORTEZZA technology for these security services, it is very important that the DON require these PKE technology related services be developed and provided as "application level" services in such a way that they are compliant with the emerging DOD "Message Security Protocol (MSP)" standards at the message/application level. In this way the DON's underlying PKE-based security services can maintain

"transparency" to underlying communications protocols, and at the same time have maximum interoperability with emerging security standards for DMS and other DoD joint systems. It is recommended that the DON embrace the MISSI/FORTEZZA technology and utilize it wherever possible to help secure internal DON network operations.

As a related area of technology investment it is critical for the DON to invest in the development and deployment of technologies which can help facilitate the protection of information which is being stored ("at rest") within operational domains. This technology should specifically be applied in protecting SBU information networks and domains as well as higher level classified infrastructures. The most fruitful technology for achieving this capability involves either software- or hardware-based embedded file encryption technology. This technology must be capable of being embedded within the individual systems at the "system bus" level and must be of sufficiently high speed in its operation that it does not unacceptably impair system performance. At this time, software-based embedded encryption techniques represent the most cost effective near-term capability for meeting these requirements. Embedded software encryption for file protection can, however, present some security risk since the encryption algorithms must be implemented using underlying operating systems which may not be high assurance and may themselves be vulnerable to penetration. The Panel believes that this risk is manageable, particularly if the application systems involved are located within protected "operational domains." The DON should select and standardize on software encryption implementations which have been reviewed by the National Security Agency (NSA) as appropriate for use in protecting information within SBU level domains, and secondly within Secret and higher level domains. The technologies and procedures developed for embedded encryption-based protection of files within systems should also be applied at the "application level" and efforts should be made to standardize encryption interfaces so as to maximize interoperability and compliance with the emerging DoD MSP standards. In this way potential costs associated with complex encryption conversion gateways can be minimized. As part of this initiative, the DON should also support the development of embedded encryption concepts to provide added levels of protection for program executables and system utilities software, and should develop a uniform encryption key management infrastructure and a key escrow strategy to support the recommended domain-level embedded encryption services.

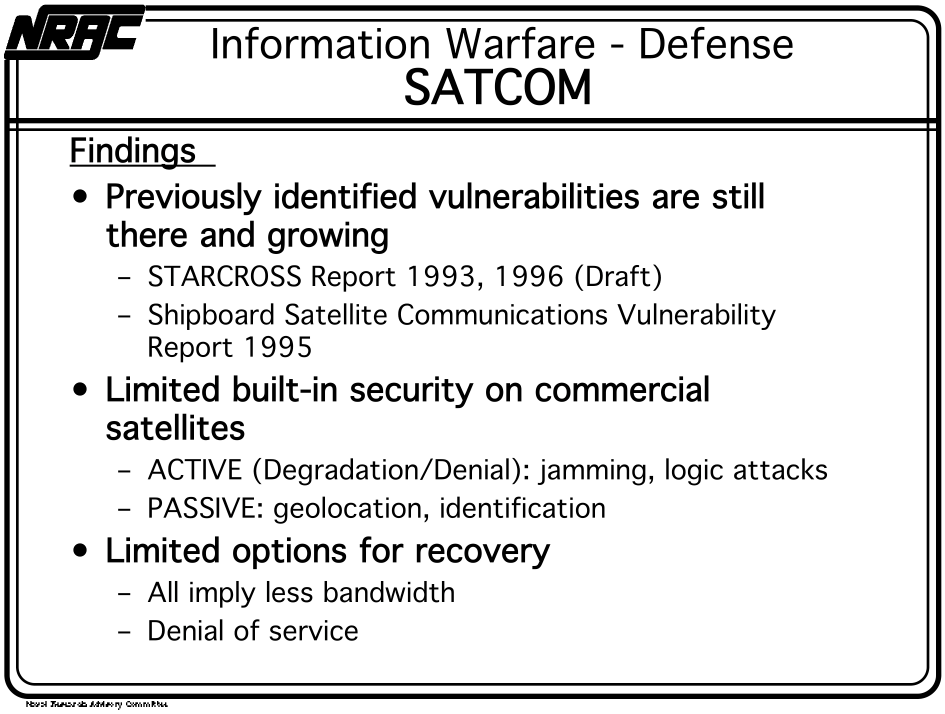


LAYERED PROTECTION TECHNOLOGIES

The DON should develop and deploy high assurance firewall and guard systems as a means of protecting and securing the perimeter of different operational domains within DON operation. These firewall and guard systems would utilize PKE-based digital signature identification and authentication technology, and would be configurable to enforce specified security and integrity policies for controlling the release and protected transfer of information between different operational "domains" as necessary. For example, the firewall/guard systems would be configurable in terms of the network level services which they would either provide as controlled proxy services, or would otherwise disallow. Included would be network services such as Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), Hypertext Transport Protocol (HTTP), and Telnet. The guard systems would also be configurable, if required, to provide additional higher "application level" security policy enforcement services related to the review and checking of data being transferred across the domain boundary. This would include, for example, "dirty word" checks, virus scans, data syntax checks, data security label checks, and other functions as required and as feasible. Depending upon the site-specific security risks involved, these firewalls and guard systems should be implemented on operating systems and platforms which have been evaluated to possess levels of implementation assurance generally in compliance with NSA's B2-level or above. This would serve to minimize the vulnerability of the firewalls/guards themselves to penetration. In

particular the DON should take advantage of proven, accredited guard and firewall systems technology already developed and fielded by the DISA Multi-Level Security (MLS) Program, as well as by the other services and by NSA.

As another critical area of network security technology investment, the DON should select, enhance and deploy a comprehensive set of network system management tools for general use by DON network administrators and managers. These would include network intrusion detection and probing tools for use in defining and evaluating network system vulnerabilities. These tools could build upon and expand currently available tools such as the Air Force ASIMS tools, the Navy's ICEPICK tools, as well as commercially available products including NET RANGER and SATAN tool sets. Efforts should be made to enhance network monitoring tools to make them as "real-time" as possible and to incorporate protective reaction capabilities as a part of these functions. The DON should also select and deploy standardized sets of more traditional network management tools as well, in order to enable network managers to monitor and control configurations and connections within their networks and sub-networks. These tools should also be enhanced to include centralized network security administration and management functions at the "domain" level including digital signature and encryption certificate authorization and other encryption key management functions. Security administration tools for configuring and maintaining firewall and guard systems as part of the "domain level" enclave should also be developed and deployed as part of the network system administrator's arsenal of tools. See page 40 for a detailed discussion of embedded encryption of data, especially data at rest.

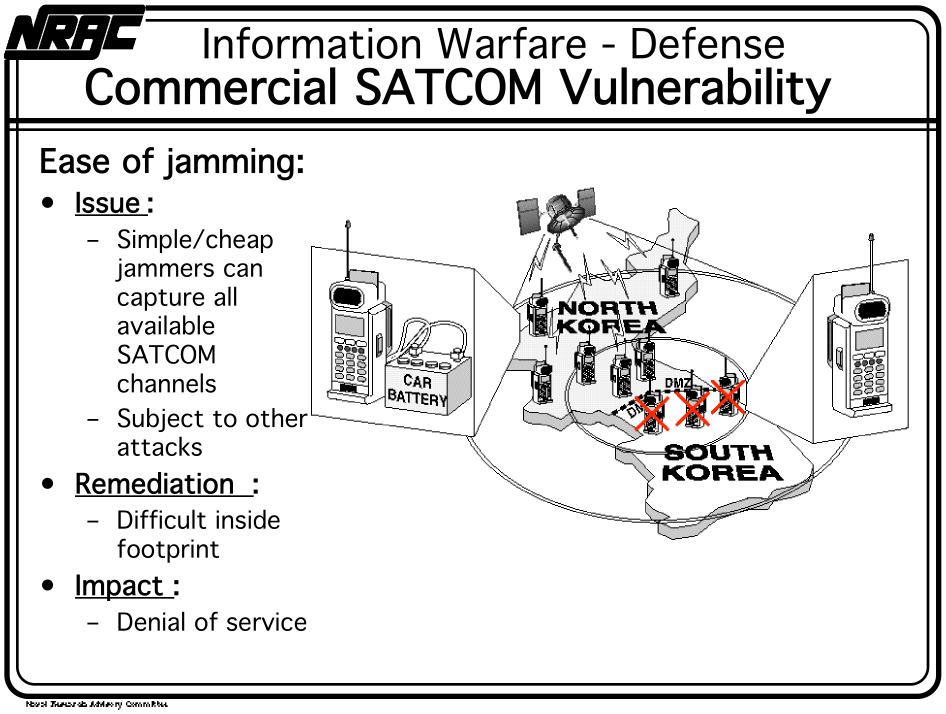


SATCOM

The fleet is the forward deployed arm of U.S. Forces. As such, it requires an open air communications capability, the requirements for which are growing at an alarming rate.

The DON and the DoD have invested heavily in military satellite technology, which provides some level of protection from denial of service and other ills of open-air transmission. These military satellites, which have provided the bulk of the communications capacity in the past, are being swamped by the recent demand for additional capability. As a response to this sharply increased demand, the DON has started to utilize the existing and rapidly developing commercial satellite infrastructure in an effort to augment its organic capability.

The commercial satellites, while seductively cost-effective and easy to use, are quite susceptible to denial of service attacks and bring with them the added danger of unwanted geolocation of the user. These vulnerabilities have been recognized by the technical community for many years (for example, the 1993 STARCROSS Report on commercial satellites and the 1995 Shipboard Satellite Communications Vulnerability study), but the Panel is concerned that the recommendations contained in these reports may not be fully appreciated, or are not being heeded in Naval operations.



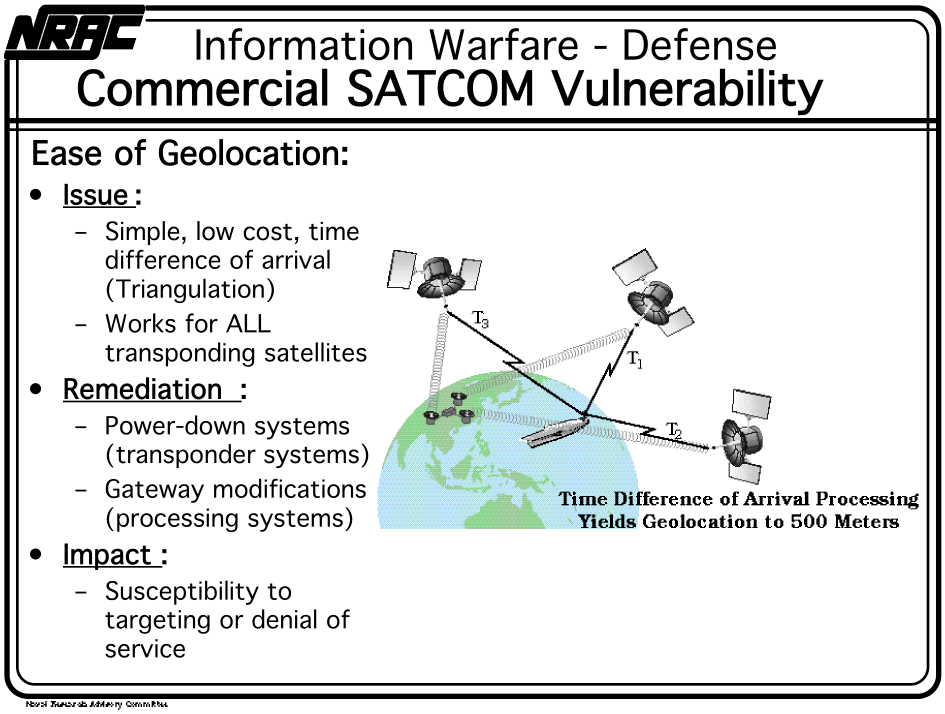
COMMERCIAL SATCOM VULNERABILITY

An important vulnerability of commercial satellites is the ease with which they can be jammed. Because of the low earth orbit (LEO), satellite receivers are designed for direct reception of the low power transmissions of personal communicators (typically less than 1 watt). The power required of a jammer for such a system is commensurably small.

The commercial systems also employ a simple control structure which make them subject to simple "spoofing" attacks such as the generation of a "hang up" code. In reality, commercial ground units may actually be used to jam the entire system with little or no modification. The cost of these jammers is on the order of the cost of the commercial ground units, typically less than $1,000, making the proliferation of a large number of jammers entirely feasible.

Placement of a suitable number of jammer units, perhaps a few hundred, anywhere within the communications satellite's antenna "footprint" (1 every 100 km^2), will jam communications within that entire footprint. Since the smallest footprint of any satellite considered by the Panel was on the order of 350 km and the largest footprint spanned half a continent, this type of attack is seen as both cost-effective and extremely difficult to mitigate.

Such a “denial of service” attack is so easily accomplished that reliable communication over commercial LEO channels should not be expected during hostilities, and the DON should make a substantial effort to minimize reliance on these devices as they become available over the next few years.



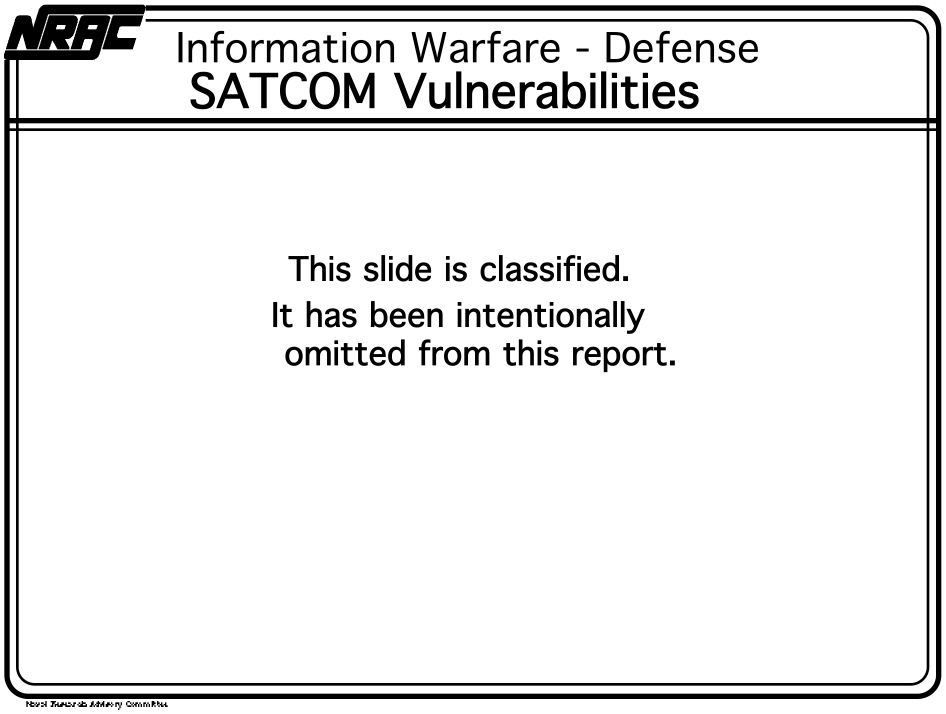
COMMERCIAL SATCOM VULNERABILITY

A second significant vulnerability of many multi-satellite communication systems is the ability to geolocate any emitting element in the system by triangulation techniques known as Time Difference of Arrival (TDOA) or Frequency Difference of Arrival (FDOA). The simplest implementation to understand is a three-satellite TDOA system in which an emission from a ground site is detected at three different times by the three different satellites, and the time differences are compared yielding a fairly precise emitter location on the surface of the earth.

There are two basic types of communications satellites with which this can be done, simple transponding satellites and satellites that employ on-board digital processing. In the on-board processing case, such as the IRIDIUM system, geolocating is done routinely and the USER ID, telephone number and address (latitude/longitude) are available in the system with the proper access. Typical advertised accuracies of these systems are on the order of 500 meters. In fact, an optional service of these systems is the ability to locate oneself on the globe with this kind of accuracy. For the processing systems, total data security is required to protect the calculated locations of emitters within the system. This implies, as a minimum, use of a dedicated gateway which assures confidentiality of user locations.

The majority of communications satellites are transponding satellites, and all of these are subject to unintended geolocation of an emitter. This is accomplished when a ground station receives and processes the signals from multiple satellites. Processing of some weak signals received in the sidelobes of the satellite antenna system may be needed to accomplish this, but such techniques are fully within the state-of-the-art on the ground. Systems to determine emitter geolocation using the technique described above have been developed for commercial use and are being sold internationally, some with an alleged accuracy of 4 km.

The only assured protection response in either of these cases is to power down the system, i.e. turn it off, since some of the SATCOM systems can be polled from orbit, unbeknown to the user on the ground.



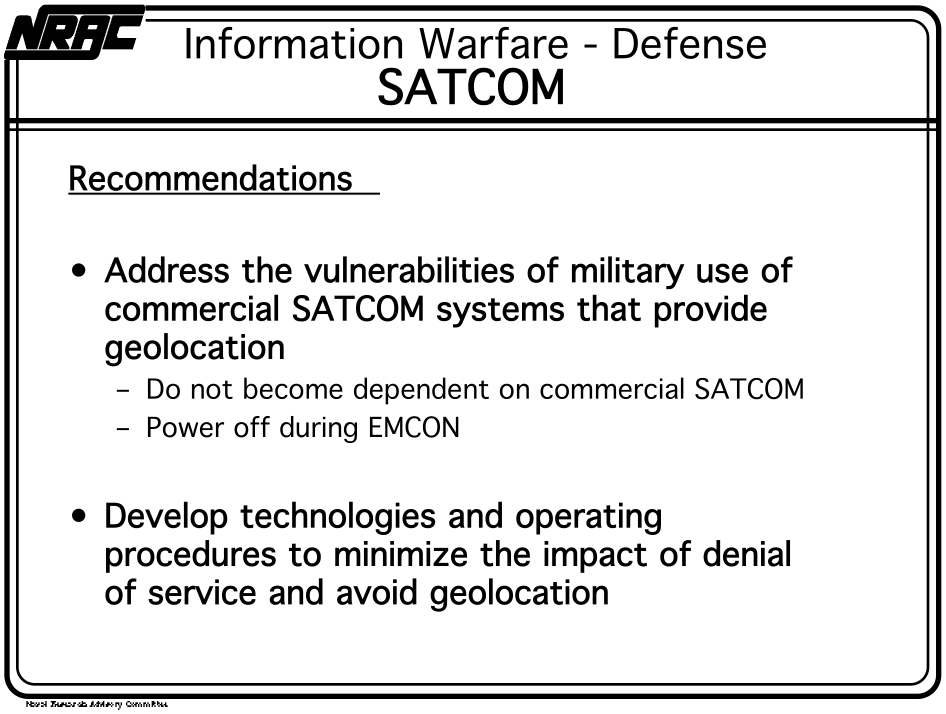
SATCOM VULNERABILITIES

Some military systems in Geosynchronous Earth Orbit (GEO) have been designed to provide an acceptable level of anti-jam capability. For these systems, denial of service is unlikely due to the high level of jamming required to defeat such a system, and the consequent vulnerability of the jammer. These satellites also provide on-board signal processing of the received signal, prior to retransmission, which serves to protect the location of the ground emitter. In general, these excellent security features have been expensive to implement and have come at the further expense of bandwidth. However, service approaching T-1 bandwidths with full duplex features will be available from these military systems within the next few years.

Commercial satellites which are very attractive from a cost and convenience point of view, and which are coming on-line soon, are far more susceptible to both denial of service attacks and unintended disclosure of geolocations of the emitter. These satellites will generally be in much lower earth orbits (LEO, MEO) thus facilitating the use of low powered SATCOM terminals for personal use. This commercially innovative feature has made these system vulnerable to low-power denial of service attacks. Furthermore, as discussed previously, the commercial transponding satellites such as GLOBALSTAR and ODYSSEY permit a ground station employing TDOA/FDOA techniques to geolocate a ground

unit; both systems routinely and automatically perform geolocation functions to aid them in space segment asset management and billing.

Commercial systems appear to be vulnerable to denial of service attacks and unintended disclosure of the geolocation of the emitter. If commercial SATCOM services are used extensively by the DON, care must be exercised that surface units are not compromised. The Global Broadcast System (GBS) will offer simplex service with large bandwidths and since it principally broadcasts from space, is not in danger of compromising the location of surface units.

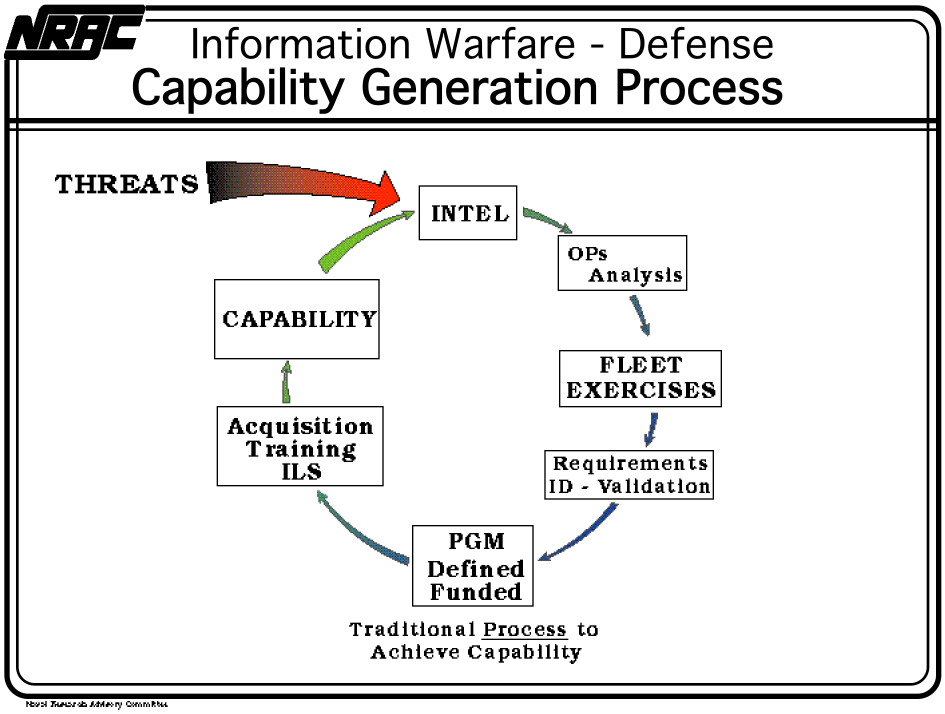


SATCOM

The Panel endorses the recommendation of the STARCROSS Report and thinks that both this and the 1995 Shipboard Satellite Communications Vulnerability Report should be required reading for all Communications officers.

It is strongly suggested that the DON develop a protocol for operating under future conditions in which commercial satellite communications are compromised or denied, and then actively train under these circumstances. Presently programmed military SATCOM systems such as MILSTAR MDR are expected to be capable of meeting projected shipboard duplex (simultaneous two-way voice and data communications) requirements for the next several years; however, the simplex (broadcast) requirements can only be met by a combination of military and commercial systems. In this latter case, provisions should be made to shed commercial bandwidth in hostile environments.

Finally, the Panel suggests that the DON develop concepts whereby the capabilities of the commercial satellite infrastructure can be utilized while at the same time the susceptibility of these systems to jamming and exploitation is minimized. For example, the use of comm-relay Unmanned Aerial Vehicles (UAV's) or towed fiber-connected relays and decoys might provide an additional layer of protection while maintaining connectivity to these cost-effective systems.

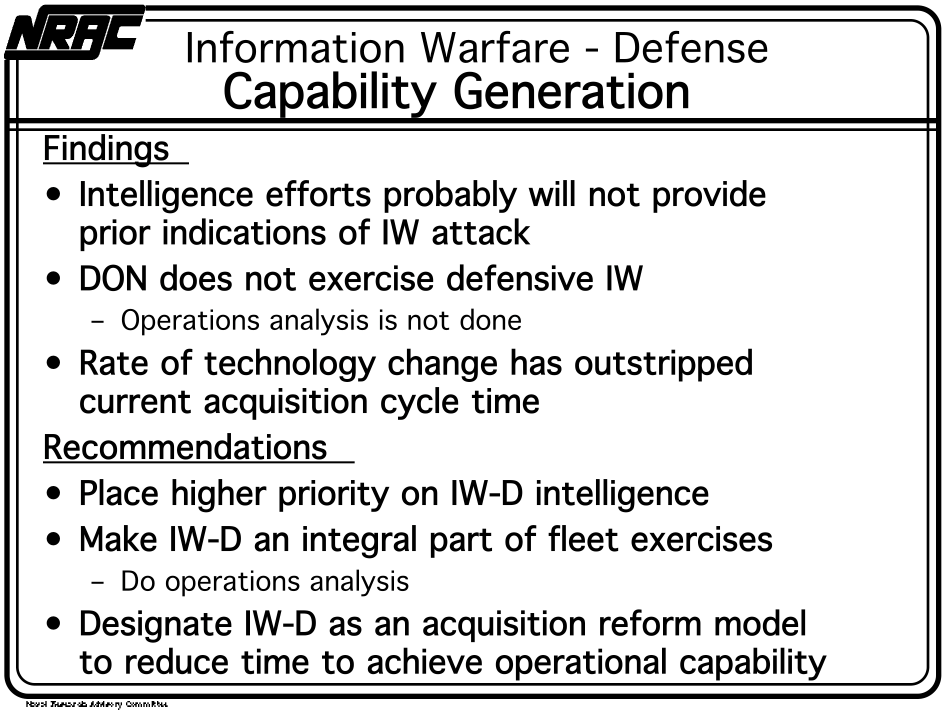


CAPABILITY GENERATION PROCESS

The process for generating operational capabilities is shown simplistically in this chart. It worked well against the old Soviet threat.

Intelligence identified a weapons system being developed; analysis was conducted of the threat presented by the weapons system; and projected capabilities were tested in war games and exercises.

As a result, programs were initiated to acquire U.S. military capabilities that defeated or effectively mitigated the threat. The resultant systems were again tested in war games and exercises. Capabilities, doctrine, tactics, procedures and techniques were developed and constantly updated. The cycle time for this process was slow, but effective, since it was well within Soviet weapons system development timelines. This process has not worked well for IW-D. It is the judgment of the Panel that fleet exercises should play an amplified role in determining IW-D needs.

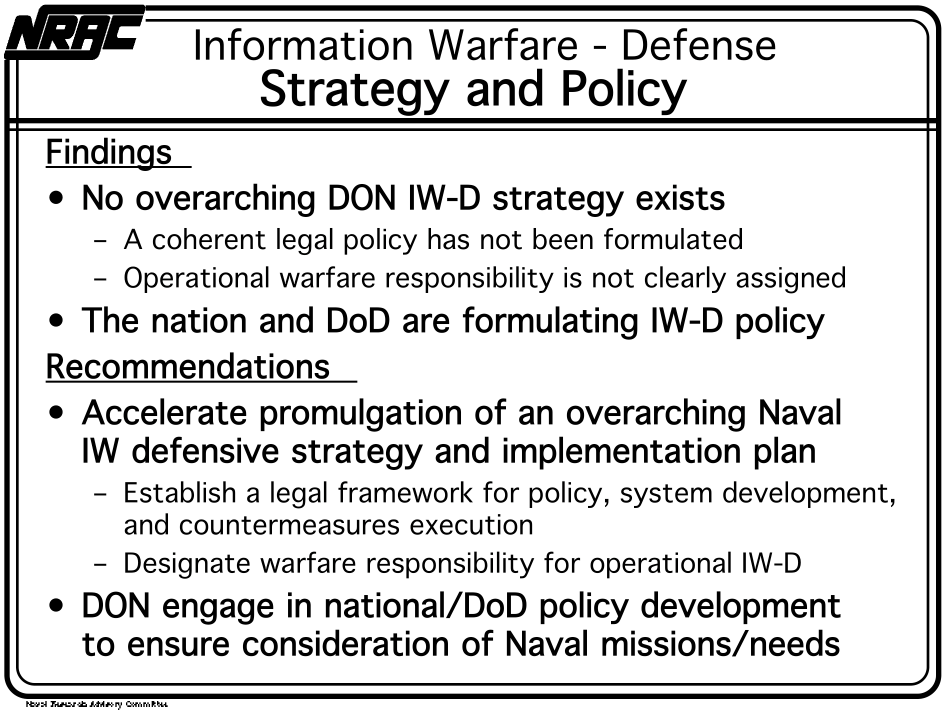


CAPABILITY GENERATION

The process for developing requirements, doctrine, tactics, techniques, and procedures is not functioning well for IW-D. Awareness of IW capabilities and threat has been constrained by compartmentalization. Although the generic intelligence threat is known, it is not yet specific enough to serve as a driver as is the case in normal systems development. There is a reluctance to exercise IW and IW-D because it could disrupt other aspects of exercises and degrade training in other vital warfare areas. Operations analysis of the impact of defensive warfare on DON command, control, and dissemination systems has not been conducted. Consequently, IW-D doctrine, requirements, tactics, techniques, and procedures have not been generated. Exacerbating this situation is the rapidity by which technological change is occurring. Traditional system acquisition timelines in excess of 5 years are no longer viable in a world where technological changes produce virtual obsolescence in systems designed only 18 months earlier. Ensuring the insertion of new technology into military systems is critical to enhancing system life and effectiveness. If the situation is not rectified, the DON will not be able to develop effective capabilities to protect its computer-based, information-based forces from becoming increasingly vulnerable to threats that could debilitate combat capability.

It is important that the DON enhance the ability of intelligence to help drive systems development. The DON's capability generation process

will be improved with IW-D as an integral part of fleet exercises. This process, in conjunction with operations analysis, is vital to ensuring that Naval systems are developed to meet fleet needs. Designation of IW-D systems to serve as an acquisition reform model can help compress traditional acquisition timelines, fielding more effective, robust, and upgradable systems in step with rapid technological change.



STRATEGY AND POLICY

Information technology has significantly improved warfighting capabilities, while at the same time exposing the military to potentially debilitating vulnerabilities. In spite of wide recognition of the information warfare threat, the DON has not issued an overarching strategy for Defensive IW. This is a mission essential deficiency. Absence of a documented strategy has resulted in fragmented and uncoordinated policy initiatives.

The national leadership is aware of the importance of information infrastructure. The increasing level of information system intrusions is bringing the vulnerability of this infrastructure to national attention. Consequently, national policy formulation has begun. The Naval information infrastructure is inextricably intertwined with the national system and will be significantly impacted by directions in national policy. During this policy formulation process, the DON has an opportunity to influence national policy, law, and objectives to enhance the security and robustness of Naval information.

A legal foundation must exist if the DON is to develop effective IW-D policy and implementing systems, and to execute countermeasures. Unfortunately, the Department has yet to develop and implement a fully coordinated legal policy. For example, warning banners are not consistently displayed on DON computer systems to warn unauthorized

intruders not to enter. The DON needs to establish a formal system that designates information system administrators and establishes their authorities. System administrators have the statutory authority to monitor their own systems, but are currently frustrated in their efforts to trace the source of intruders and discern an attack from an intrusion or a crime in a timely manner. Laws which protect privacy and property interests, and jurisdiction concerns of nations and states, limit active IW-D of the DON infrastructure.

IW attacks will target the weakest systems or organizations in a network. Without in depth defense, an effective attack will flow unimpeded into every command element having a devastating impact. Consequently, all organizations are responsible for defense and all are vulnerable. Response to an attack can be a highly complex process. The determination of the source of attack, its impact, and how best to respond are technically challenging problems that must be executed quickly and involve many command elements. Concurrently, system degradation must be traded against loss of connectivity, data integrity, and immediate situational awareness. Failure to respond well will reduce combat capability dramatically.

It is essential that the DON develop an overarching defensive IW strategy. The strategy should include the DON's guiding principles for:

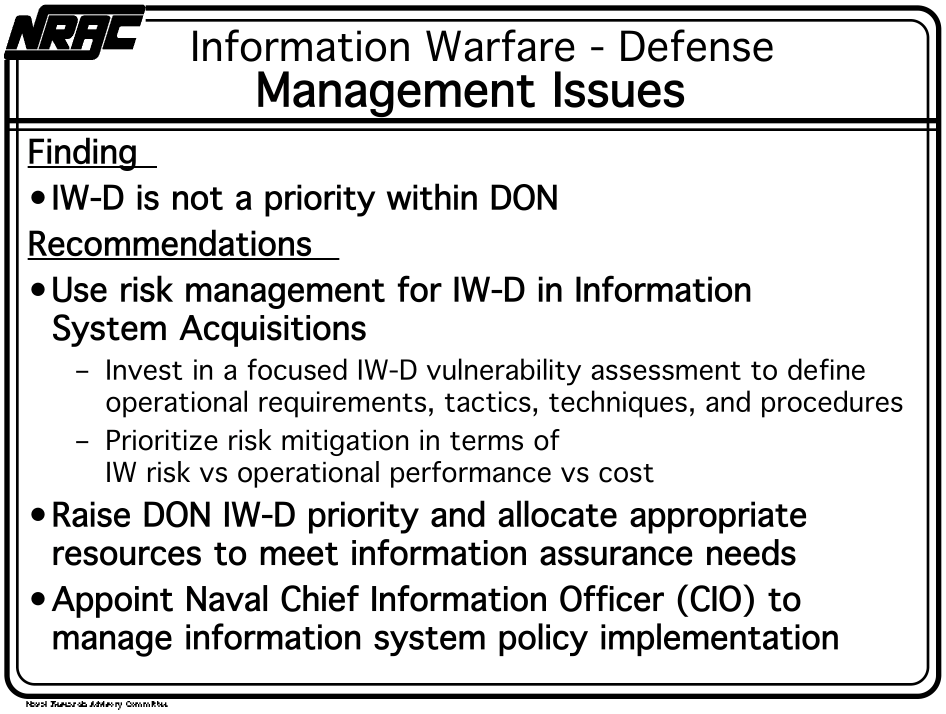
Vision	Exercises
Policy and Doctrine	Acquisition Strategy
Organization (Roles and Responsibilities)	Operating Procedures
Vulnerability Assessments	Legal
Research and Development (Technology)	Training and Education Career Development

A detailed roadmap or implementation plan needs to be developed and promulgated throughout the DON.

The DON must also engage as a full partner in policy development with the DoD and national leadership to ensure consideration of Naval missions and needs. A necessary component of both strategy and policy is a legal framework for system development and countermeasure execution. Legal concerns, including privacy, national security, law enforcement and the principles of international law, need to be integrated into policy statements and guidance to systems administrators and fleet operating commands.

A focal point to assist in DON policy development and liaison with DoD and national policy makers would be the DON's CIO. The designation of a warfare responsibility for operational IW-D is recommended as critical to effective IW-D.

In order to apply the DON's finite resources most effectively, critical DON systems need to be identified and priority given to them for implementation of IW-D.



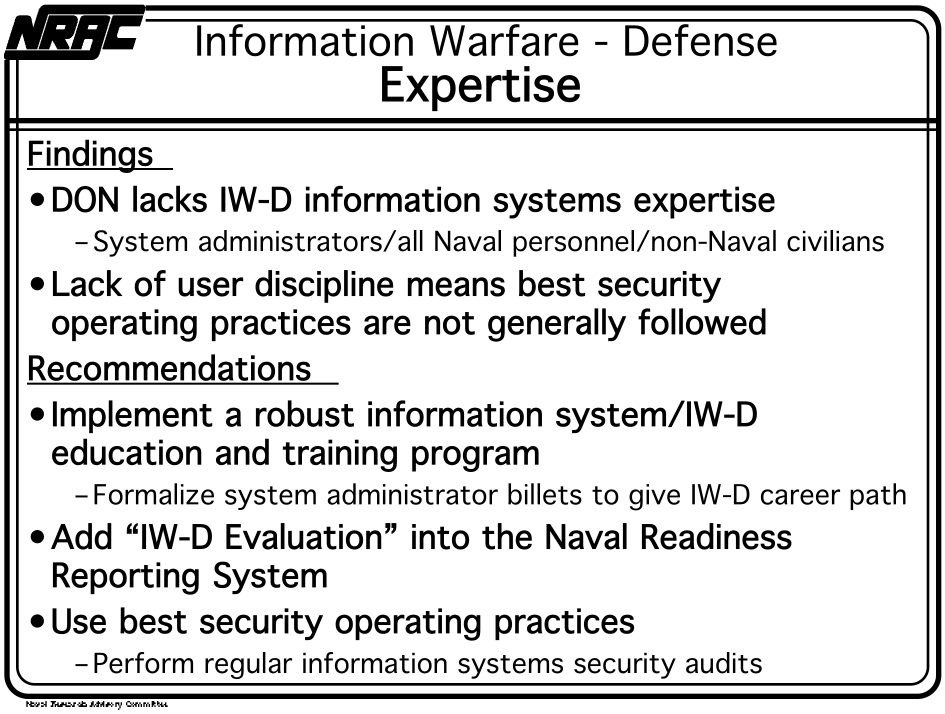
MANAGEMENT ISSUES

Traditional information system acquisitions have given modest deference to total security awareness in the definition of system requirements. Additionally, the rapid growth of global inter-networked systems has exposed systems to an environment not previously considered. Vulnerability of Naval networks has not been fully addressed and Naval forces are not fully aware of infrastructure shortfalls. Since Naval forces will continue to build their dependence on information systems and information flows, a coherent new approach is needed to ensure rapid fielding of systems, while simultaneously embedding acceptable levels of security in these acquired systems. An organizational structure needs to evolve to address DON-wide information assurance and appropriate resources need to be applied.

The CIO should be designated the DON focal point for information systems policy implementation to oversee and coordinate a coherent Naval information technology effort. It is critical to ensure that networks, both afloat and ashore, are integrated into a coherent interactive Naval network that can meld seamlessly into a joint force operation. Vulnerabilities need to be assessed to support identification of system requirements. Risk management principles, when applied to information systems acquisition, can reconcile what are viewed as two competing objectives, i.e. operational performance versus IW risk. In fact, intelligent efforts to enhance information assurance can provide the warfighter with

information of higher quality and greater integrity, within responsive timelines. Requirements need frequent periodic review, and development should be based on vulnerability assessments that take advantage of robust modeling and simulation efforts. Defensive IW risk analyses should be performed that identify operational, tactical, and material risks. As program development proceeds, conscious risk analysis tradeoff studies among information risk versus operational performance versus cost versus schedule should be performed. Alternatives reflecting these tradeoffs should be presented to the acquisition executive.

Priority must be raised for security of information systems and appropriate resources should be applied for information assurance, based on the risk management decisions that are made.



EXPERTISE

The DON needs to educate and train all personnel regarding the nature of IW and appropriate countermeasures. A number of vulnerabilities are evident. Among Naval personnel at all enlisted grade and officer levels there is a lack of understanding of the technologies, considerable lack of sophistication in the use of computer passwords, a lack of awareness of the potential of hackers to access the classified and unclassified networks via inadvertent actions of Naval personnel, and of the dangers associated with hostile or mischievous acquisition of military computer information. In addition, there is no general awareness of the vulnerability to geolocation that is associated with the use of some personal communications devices. A basic training IW component (module) and inclusion of IW-D in overall unit security training would address these problems. Officer awareness and understanding of the technologies would be facilitated by including IW-D evaluation into the Naval readiness reporting system.

System operators are believed to be responsible for the bulk of the problems related to detection and recognition of computer-related intrusions into military systems. In addition to the above training and education issues, they need data information systems that utilize a series of operating procedures that provide additional levels of confidence to protect against current and future intrusions and exploitation. Operating procedures that address the basic protection of electronically

stored data, access to the data storage and critical system utilities software, and communications to and from mass storage equipment can all be implemented in a cost efficient manner.

The most effective methods for secure operating procedures are immediately available and can be implemented with general instructions not presently being followed. Examples include: diligent password usage, changing system default settings, basic personal attention to the design of a password and conscious security monitoring of the workplace.

The need for more and better trained systems administrators is serious. The job is presently defined as additional collateral duty for junior enlisted personnel and officers outside of the primary Navy Enlisted Code (NEC)/ Designator specialties. System Administration is without a career path. Appropriately trained system administrators are prime candidates for higher paying job offers from the private sector and are therefore difficult to retain in the DON.

Numerous non-military personnel, i.e. contractors and/or civilian employees of the Navy and Marine Corps, are involved in shipboard and shore operations. There is no mechanism at present for assuring the DON that they possess a level of awareness and training sufficient to qualify them in the IW-D arena.

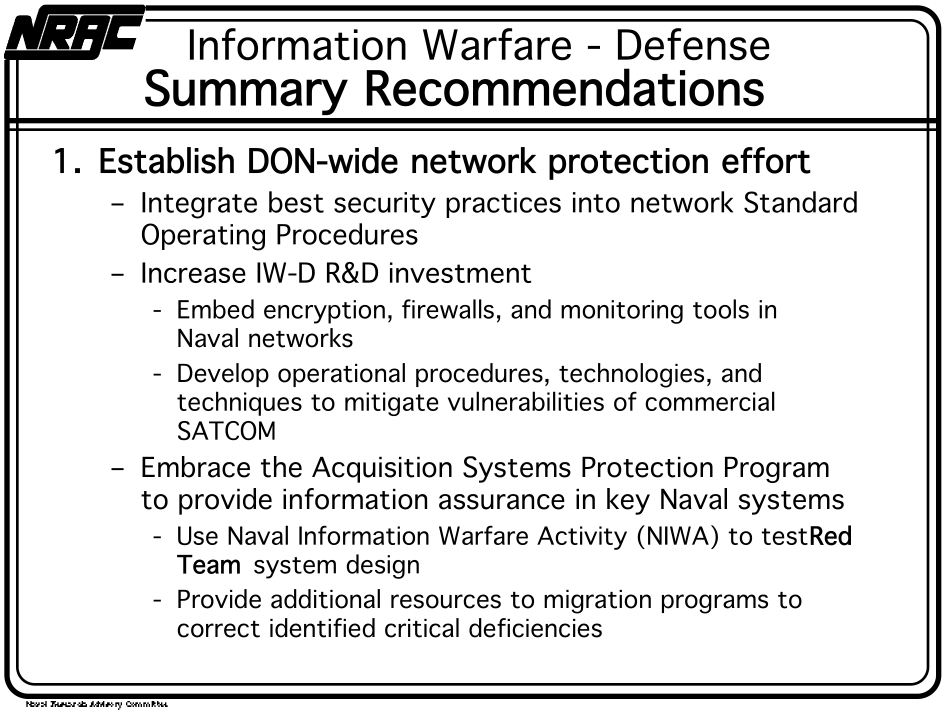
There are readiness issues in all of the above that education and training, together with tightened operating procedures, can repair.

The degree to which intrusions into military information systems are related to the lack of understanding of these systems and their vulnerabilities on the part of Naval personnel, particularly system administrators, call for early remedial action. Early implementation of robust training and education programs is strongly recommended.

The dependence of the DON on the competence of a sufficient number of system administrators and the difficulty in retaining these individuals argues strongly for more system administrator billets and the establishment of a motivating career path in IW-D.

Addition of an IW module into the Navy's A school, together with the addition of IW-D evaluation into the Naval Readiness Reporting System, is recommended. The intent is to provide motivation for personnel at all levels and degrees of experience to obtain and retain the competence required to execute the DON's missions.

A system of awareness, information system functions, and risk management principles should be initiated at all personnel levels. The institution of clear and concise procedures is urgent.



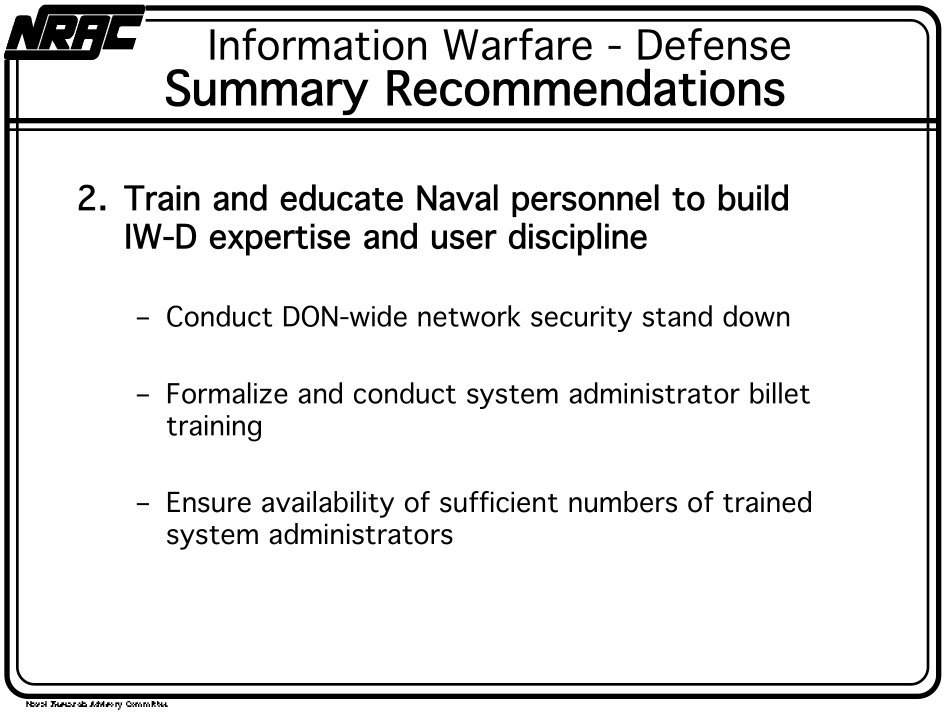
SUMMARY RECOMMENDATIONS

This last decade's tremendous growth in command, control, communications, computers, intelligence and reconnaissance has provided the U.S. Navy and U.S. Marine Corps with great tactical and strategic advantages. The new doctrine and systems are absolutely dependent upon a knowledge advantage, and therefore upon information. For example, maneuver warfare, cooperative engagement, bomb damage assessment and precision guided munitions are not viable without timely accurate information. Naval forces will be blind and deaf if IW-D is not effective.

In order to maintain a knowledge advantage, there is great pressure to develop and deploy advanced state of the art information systems. For valid reasons, much of the hardware and software acquired is commercial off the shelf technology (COTS). This equipment is not designed to meet military security requirements, and thus, unfortunately, it is not inherently secure. Consequently, a great deal of the information technology currently delivered to operational units has significant security weaknesses. For this reason, a network protection effort, including systems research and development, must be established to assure levels of protection commensurate with evolving information technology.

Many of the systems' weaknesses could be significantly mitigated at low cost. Setting up Red Teams to test system design during the

acquisition process will ensure that actions are taken to correct critical deficiencies. It is the Panel's understanding that the Naval Information Warfare Activity (NIWA) has been designated to "Red Team" system design.

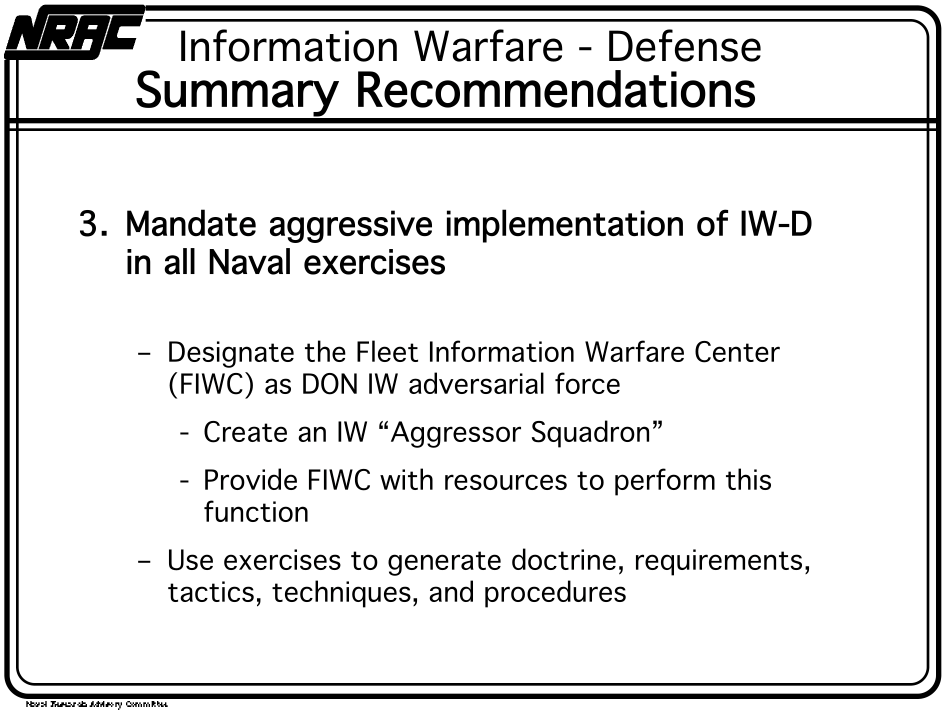


SUMMARY RECOMMENDATIONS

As in any aspect of warfare, motivation and skill are extremely important. This is especially true in the IW-D business. Today there is a general lack of understanding among Naval personnel, at all levels of the technologies and potentials for exploitation associated with information warfare. The Panel recommends an early DON-wide network security stand-down to provide the necessary breadth of awareness of existing vulnerabilities.

Today, sufficient numbers of trained people are not in position to properly administer and protect DON networks. In addition, there is no system that emphasizes the DON's need to retain personnel with the requisite skills.

As sophisticated network protection tools are employed, the requirement for skilled personnel will increase. The DON needs to train and educate its people and provide for career motivation.

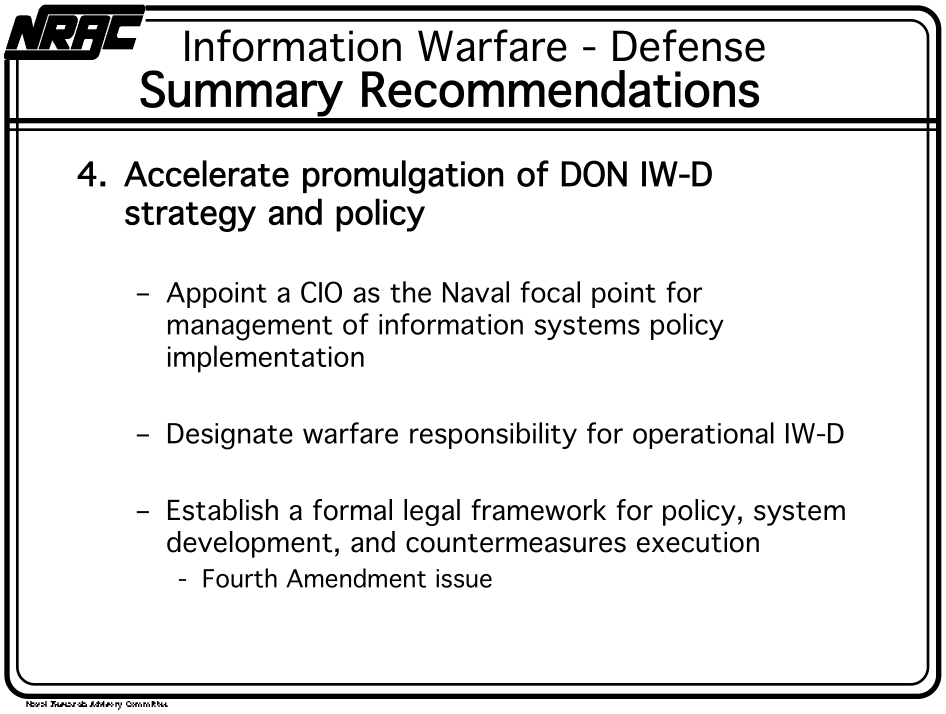


SUMMARY RECOMMENDATIONS

Once IW-D systems become operational, it is mandatory that vulnerabilities are understood and that best operating procedures are implemented. Exercises will likely be the prime source for initiatives, requirements, doctrine, procedures, tactics, and techniques.

Fleet exercises that include aggressor force challenges to *in situ* assets, practices and operational procedures are instrumental in formulating a robust set of IW-D requirements and plans of action. IW-D must be exercised in order to jump start the entire process.

It is the Panel's understanding that the Fleet Information Warfare Center (FIWC) has been chartered to participate in fleet training. Together with NIWA in its designated Red Team role in system design, the FIWC role as aggressor force in operational exercises will significantly enhance the Navy's IW-D posture. Both NIWA and FIWC are well suited to perform these functions; but are only just starting to provide the required support. Their contributions could be significantly enhanced with modest resource increases, some mission expansion and more command attention to IW-D.



SUMMARY RECOMMENDATIONS

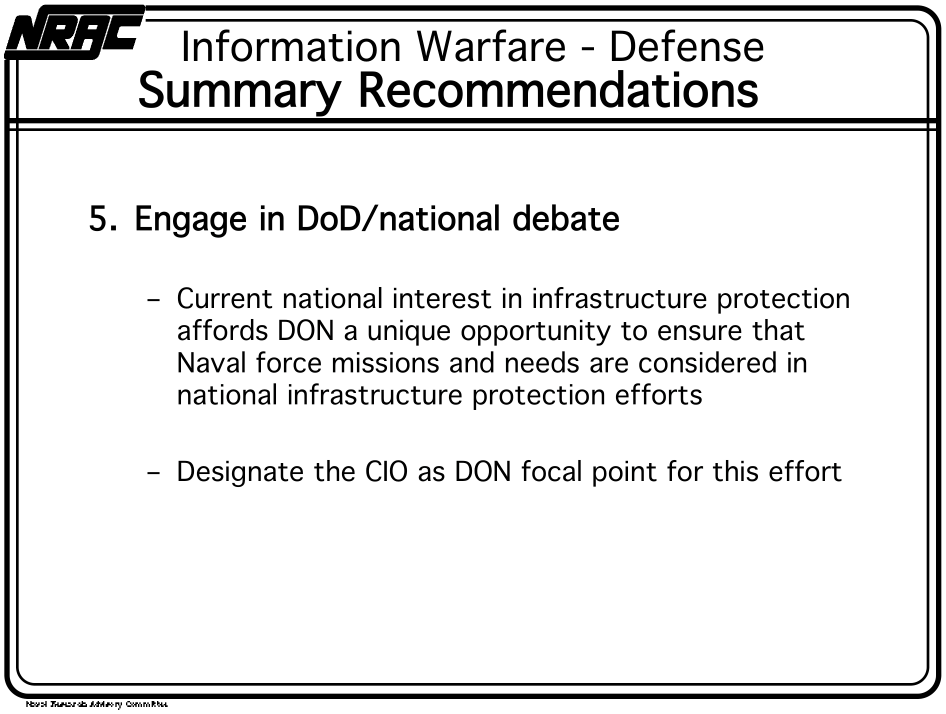
This is one of the easiest and yet most important recommendations.

The CIO recommended by the Panel should report to the Office of the Secretary of the Navy and should serve as the focal point for DON policy, plans and implementation.

Operational warfare responsibility for IW-D needs to be clearly assigned.

A legal framework is necessary for the use of certain new technologies for IW-D system defense. In particular, legal policy regarding response to intruders is necessary for system administrators. Lack of precedent-setting law in this area requires active Naval legal participation in the debate regarding formulation of new laws.

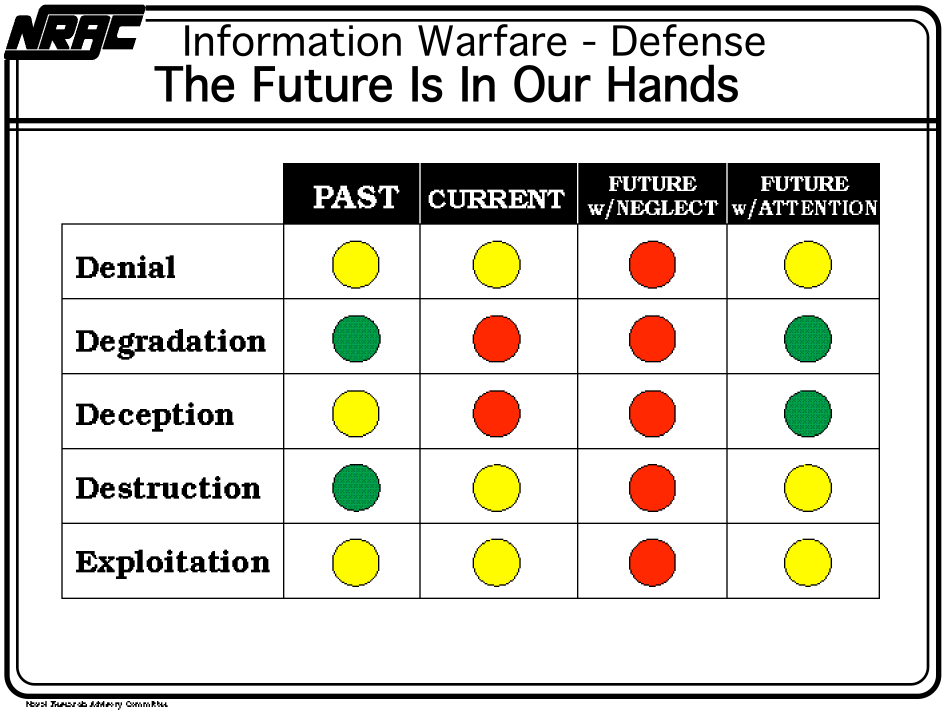
Almost all of the documentation required exists in draft form. The material looks like an excellent start to the Panel, but it needs to be completed, soon.



SUMMARY RECOMMENDATIONS

The national debate which is currently ongoing will result in policy which will ultimately impact Naval combat capabilities. The DON must be a full partner in order to assure full consideration of its mission and needs. Responsibility for its own policy development and for DON liaison with national policy makers, including those of the DoD, must be designated. The Panel recommends that warfare responsibility for operational IW-D within the DON be vested in a CIO and that this individual be identified at the earliest possible time.

What is important to the DON must be decided and those issues proactively pursued.



THE FUTURE IS IN OUR HANDS

Earlier pages of this report have described the past and current status, along with the concerns of the Panel that relate to potential compromises of information systems.

As always, the future is in our hands.

If the IW-D issue is accorded benign neglect, the future is grim.

The Panel feels strongly that if action is taken now and the issues raised here are addressed, an acceptable level of security can be obtained at what appears to be a reasonable cost.

Appendix A: Acronym List - NRAC Information Warfare Report

AIS	Automated Information System
A-J	Anti-Jamming
ARG	Amphibious Ready Group
C^4I	Command, Control, Communications, Computers, and Intelligence
CINC	Commander-in-Chief
CIO	Chief Information Officer
COMINT	Communications Intelligence
COTS	Commercial-off-the-Shelf
CVBG	Carrier Battle Group
DCI	Director of Central Intelligence
DEPSECDEF	Deputy Secretary of Defense
DISA	Defense Information Systems Agency
DISNET	Defense Information Systems Network
DMS	Defense Message System
DoD	Department of Defense
DON	Department of the Navy
EMCON	Emission Control
EW	Electronic Warfare
FDOA	Frequency Difference of Arrival
FIWC	Fleet Information Warfare Center
FMI	Foreign Military Intelligence
FTP	File Transfer Protocol
GAO	General Accounting Office
GBS	Global Broadcast System
GEO	Geosynchronous Orbit
HTTP	Hypertext Transport Protocol
IW	Information Warfare
IW-D	Information Warfare - Defense
JMCIS	Joint Maritime Command Information System
LAN	Local Area Network
LEO	Low Earth Orbit
LOS	Line of Sight
MBPS	Megabits per Second
MEO	Medium Earth Orbit
METOC	Meteorological and Oceanographic Information
MLS	Multi-Level Security
MSP	Message Security Protocol
MWR	Morale, Welfare and Recreation
NEC	Navy Enlisted Code
NIWA	Naval Information Warfare Activity

NRAC	Naval Research Advisory Committee
NSA	National Security Agency
PKE	Public Key Encryption
R&D	Research and Development
RF	Radio Frequency
SATCOM	Satellite Communications
SBU	Sensitive-But-Unclassified
SIGINT	Signals Intelligence
SIPRNET	Secret DOD Internet
SMTP	Simple Mail Transfer Protocol
TDOA	Time Difference of Arrival
UAV	Unmanned Aerial Vehicle
WAN	Wide Area Network