Executive Summary
Information Warfare - Defense

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.