Executive Summary
Information Technology Interoperability

Purpose of the Study

Recognizing the information technology explosion, the impact on the Department of the Navy (DON), and the need to provide for Joint Force Interoperability with allied and coalition forces, the Assistant Secretary of the Navy for Research, Development and Acquisition [ASN(RD&A)] asked the Naval Research Advisory Committee (NRAC) to convene a panel to assess Information Technology (IT) Interoperability Among Systems, with a Focus on Allied and Coalition Warfare. The Panel focused its attention on the current plans and strategies for interoperability, and identified both currently perceived impediments and mitigation plans. Included was an assessment of current and near-term technology to enable secure interoperability. The Panel also focused on providing recommendations for both policy and technical actions to mitigate currently identified impediments to achieve and maintain those levels of interoperability required to support execution of Naval missions in a joint/NATO/Allied/coalition force environment. The Panel feels that this report can serve as the basis for an affordable DON investment strategy and roadmap for achieving the levels of information technology interoperability required.

Framework and Approach

The operational nature of the study required significant background knowledge. Accordingly, subject matter experts were invited to join the Panel. Conceptual and operational frameworks were established based upon a working definition of information technology interoperability and discussions with several, in-place, fleet command Flag officers to establish a current benchmark and to understand their concerns. The definition derived for the study is "the *timely* exchange of sufficient information among *operational elements* (joint, NATO, allied, coalition) to successfully *plan, coordinate* and *control* assigned missions." It is, perhaps, equally as important to identify that the Panel did not address interoperability as it extends to that level of complexity required for weapons and combat control functions.

The Panel addressed a number of plans, policy, procedural, and technology issues during its deliberations, based upon briefings and interactions within the wide-based IT and operational communities. There was a discrete set of issues, isolated by the Panel, which were determined to be study "drivers." Findings were sorted into those relevant to plans and procedures, and those relevant to technology. Recommendations were determined to correspond to each specific area. A set of overall strategies and recommendations was derived based upon the findings and recommendations in each area and within the context of those issues determined to be study drivers.

"Take Aways"

The Panel boiled this down into three overarching issues and three overarching recommendations that they believe should be considered as immutable, or "take aways" from the study. The three issues are: 1) US Forces must operate with NATO, Allied and coalition forces; 2) the DON must continue to promote network technology (e.g. IT-21); and 3) classified information must be protected. The Panel offered three overarching recommendations that apply across the board to these issues: 1) appoint a single authority; 2) establish, for interoperability, a Virtual Operations Network (VON) architecture; and 3) demand interoperability in acquisition/ training/doctrinal processes. Expansion of these issues into a summary set of strategies and recommendations follows a description of those elements found to be study "drivers."

Study Drivers

In the course of the Study, the Panel determined that there are a number of "drivers" in the field of IT Interoperability. These formed the basis for the study and subsequent development of strategies and recommendations.

The US is the global leader in the IT industry, and the US Military will continue to push technology solutions toward improving communications, command and control, computers, intelligence, surveillance and reconnaissance capabilities (C4ISR) to make its forces more efficient and effective. This is articulated in "Joint Vision 2010."

The US will continue to seek the benefit of Joint Force, allied and coalition operations to provide maximum leverage. Interoperability among these forces is paramount.

Each partnerþs classified information assets must be protected, as information is shared during mutually supported operations. All levels of networking among partners must provide this protection, adding stress to IT interoperability.

New initiatives to capture the full benefit of IT growth, such as "Network Centric Warfare," emerging from IT-21 will continue to stress interoperability.

Interoperability with coalition partners provides a further stress upon the system, since coalition partners may only be known on an ad hoc basis as the partnership unfolds for a particular military objective.

Differences in capability, technology, or applications embedded within operations are certain to exist for the individual forces which may participate in allied and coalition operations.

Three elements thus emerged as a study baseline: 1) identity of the coalition partners is not known a priori; 2) information infrastructures are unequal; and, 3) information interoperability is minimal.

Plans and Procedures

The Panel found that many of the obstacles that mitigate against achieving seamless interoperability with allied and coalition forces are rooted in policy and management procedures. Differing national interests that govern security and releasability issues, provide differing Command, Control, Communications, Computers and Intelligence (C4I) structures, and a number of different bilateral agreements between countries is endemic to the problem. The Panel found no single well-defined authority, or chain-of-command, in charge of interoperability. Systems are often not designed with interoperability in mind, nor is interoperability verified before fielding. The Panel also found inadequate emphasis on interoperability during training and fleet exercises. The Panel found many directives, instructions, and regulations that address interoperability but found them to be lacking in terms of clarity, enforcement, and integration of activities to achieve interoperability. Procedures that could be enhanced include those affecting doctrine, experiments, demonstrations, exercises, education and training, certification, technology transfer, and security/releasability.

Technology

The Panel found several technical obstacles to interoperability. Most of the technical obstacles appeared to fall within the realm of unequal capability among prospective partners; including networks, bandwidth, satellite communications (SATCOM), and command and control (C2) applications. US, NATO and allies/coalition movement to commercial off-the-shelf (COTS)-based network centric information systems is not coordinated. Mobile naval "afloat" operations present a unique problem that has led to a dependence upon SATCOM as a necessary infrastructure element to support information exchange. Current Ultra High frequency (UHF) SATCOM capabilities do not provide adequate bandwidth. New operational concepts that combine bandwidth and enhanced UHF SATCOM capability with the downlink capability of Global Positioning System (GPS) could provide enhanced information interoperability. Common needs include interoperative high frequency (HF) and SATCOM with common frequency allocation, low profile antennas, mitigation of SATCOM vulnerabilities, and bandwidth and information security. Finally, the Panel believes that it may be fruitful to provide software-based data format translation tools for critical operations that require interoperability.

Details of the recommended interoperability VON are provided in the body of the report. The recommended capability should include Transport Control Protocol/Internet Protocol (TCP/IP) Network compatibility, video teleconferencing, bandwidth on demand, Global Broadcast System (GBS) interfaces, automated message and language translators, and Public Key Encryption Infrastructure (PKI) security services.

Summary Strategies and Recommendations

TFour distinct "strategies" emerged, based upon IT interoperability issues, as shaped by relevant DON interests. The four strategies, with their accompanying recommendations grouped below, are outlined here:

- **US Forces must operate with NATO, Allied and coalition forces**
    - ASD(C^4ISR) designate a single US authority to be proactive on interoperability issues with NATO, allied and coalition forces
    - DASN(C^4I)/OPNAV N6/MCCDC should actively participate in all NATO interoperability fora
    - DON CIO appoint a Deputy to focus on NATO, Allied and coalition interoperability
- **Continue to promote network technology**
    - SPAWAR establish, demonstrate and refine an interoperability VON capability
    - OPNAV N8/MCCDC fund critical enabling technologies such as UHF SATCOM, PKI, high assurance guards
    - Systems Commands (SYSCOMS) insert hardware/software by open system architecture approaches
- **Protect classified information**
    - ASD(C^4ISR) utilize PKI technology
    - DASN(C^4I) adopt and enhance high assurance, programmable guard technology
    - ASD(C^4ISR) adopt the Secret and Below Initiavive (SABI) process for effective security/releasability procedures
- **Demand interoperability in the Acquisition/Training process.**
    - ASN(RD&A) modify acquisition process to emphasize interoperability issues at milestone reviews
    - SYSCOMS enhance the technology refresh cycle with interoperability verified for each update
    - Commanders in Chief (CINCs) promote international exercises/training and OPNAV/ MCCDC ensure feedback to the acquisition system
    - ASD(C^4ISR)/DISA enforce interoperability and certification requirements.

The Opportunity

If the DON focuses on the Key Take Aways -- 1) appoint single authority; 2) establish a VON architecture; 3) demand interoperability in acquisition/training/doctrinal processes, through implementation of the four strategies and recommendations, the opportunity is . . .

A guaranteed known level of interoperability with NATO, Allied and coalition partners - soon!