



UNCLASSIFIED

Naval Research Advisory
Committee Report



Information Technology Interoperability

November 1998

DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS
ONLY TO PROTECT INFORMATION FROM AUTOMATIC DISSEMINATION AS OF 1 NOVEMBER
1998. FURTHER DISSEMINATION OF THIS DOCUMENT IS AUTHORIZED ONLY AS DIRECTED
BY THE NAVAL RESEARCH ADVISORY COMMITTEE.

OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and manipulating the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office Management and Budget Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)		2. REPORT DATE October 1998		3. REPORT TYPE AND DATES COVERED Final, March - October 1998	
4. TITLE AND SUBTITLE Information Technology Interoperability with NATO and Coalition Forces				5. FUNDING NUMBERS	
6. AUTHOR(S) K. Hegmann, T. Brancati, L. Hettche, J. McConnell, S. Sears, J. Sinnett, K. Smith, R. Spindel, G. Webber, R. Wilson, G. Windsor					
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Research Advisory Committee 800 North Quincy Street Arlington, VA 22217-5660				8. PERFORMING ORGANIZATION REPORT NUMBER NRAC-98-02	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Assistant Secretary of the Navy (Research, Development and Acquisition) 1000 Navy Pentagon Washington, DC 20350-1000				10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES					
12a. DISTRIBUTION/AVAILABILITY STATEMENT Distribution authorized to U.S. Government agencies and their contractors only to protect information from automatic dissemination as of 31 October 1998. For additional copies, contact the Naval Research Advisory Committee.				12b. DISTRIBUTION CODE	
13. ABSTRACT (Maximum 200 words) NRAC assessed information technology interoperability among systems, with a focus on allied and coalition warfare. Specifically, the study addressed current interoperability plans and strategies, identified perceived impediments and mitigation plans, and assessed technology for enabling secure interoperability. Recommendations included policy and technical actions for mitigating impediments, and achieving and maintaining the interoperability levels required to support Naval missions in a joint/NATO/Allied/coalition force environment. The study did not address interoperability issues for weapons and combat control functions. Three observations were made: 1) identity of coalition partners is not known <i>a priori</i> ; 2) information infrastructures are unequal; and, 3) information interoperability is minimal. Most technical obstacles were associated with unequal capability among prospective partners, including networks, bandwidth, satellite communications, and command and control applications. US, NATO and allies/coalition movement to commercial off-the-shelf (COTS)-based network centric information systems is not coordinated. Three overarching issues and recommendations were identified: 1) US Forces must operate with NATO, Allied and coalition forces; 2) DoN must continue to promote network technology; and 3) classified information must be protected. Three recommendations apply: 1) appoint a single authority; 2) establish for interoperability a Virtual Operations Network (VON) architecture; and 3) demand interoperability in acquisition/training/doctrinal processes.					
14. SUBJECT TERMS: Interoperability; information technology; NATO; Allies; coalition forces; Naval missions; information infrastructures; networks; bandwidth; satellite communications; command and control; commercial off-the-shelf (COTS); acquisition; training; doctrine				15. NUMBER OF PAGES 102	
				16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT None		

NSN 7540-01-280-5500

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT NUMBER October 1998		2. REPORT TYPE AND DATES COVERED Final March - October 1998	
3. AUTHOR(s) K. Smith, R. Spauld, G. Weibler, R. Wilson, O. Windsor, R. Hargrave, T. Grant, L. Heltzer, J. McConnell, S. Smith, J. Stines		4. TITLE AND SUBTITLE Information Technology Interoperability with NATO and Coalition Forces	
5. AUTHORING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Research Advisory Committee 500 North Quincy Street Arlington, VA 22217-5000		6. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Research Advisory Committee 500 North Quincy Street Arlington, VA 22217-5000	
7. AUTHORING ORGANIZATION REPORT NUMBER NMAC-98-02		8. PERFORMING ORGANIZATION REPORT NUMBER NMAC-98-02	
9. PERFORMING ORGANIZATION REPORT NUMBER NMAC-98-02		10. PERFORMING ORGANIZATION REPORT NUMBER NMAC-98-02	
11. DISTRIBUTION STATEMENT Unrestricted			
12. DISTRIBUTION STATEMENT Unrestricted			
13. DISTRIBUTION STATEMENT Unrestricted			
14. DISTRIBUTION STATEMENT Unrestricted			
15. DISTRIBUTION STATEMENT Unrestricted			
16. DISTRIBUTION STATEMENT Unrestricted			
17. DISTRIBUTION STATEMENT Unrestricted			
18. DISTRIBUTION STATEMENT Unrestricted			
19. DISTRIBUTION STATEMENT Unrestricted			
20. DISTRIBUTION STATEMENT Unrestricted			
21. DISTRIBUTION STATEMENT Unrestricted			
22. DISTRIBUTION STATEMENT Unrestricted			
23. DISTRIBUTION STATEMENT Unrestricted			
24. DISTRIBUTION STATEMENT Unrestricted			
25. DISTRIBUTION STATEMENT Unrestricted			
26. DISTRIBUTION STATEMENT Unrestricted			
27. DISTRIBUTION STATEMENT Unrestricted			
28. DISTRIBUTION STATEMENT Unrestricted			
29. DISTRIBUTION STATEMENT Unrestricted			
30. DISTRIBUTION STATEMENT Unrestricted			
31. DISTRIBUTION STATEMENT Unrestricted			
32. DISTRIBUTION STATEMENT Unrestricted			
33. DISTRIBUTION STATEMENT Unrestricted			
34. DISTRIBUTION STATEMENT Unrestricted			
35. DISTRIBUTION STATEMENT Unrestricted			
36. DISTRIBUTION STATEMENT Unrestricted			
37. DISTRIBUTION STATEMENT Unrestricted			
38. DISTRIBUTION STATEMENT Unrestricted			
39. DISTRIBUTION STATEMENT Unrestricted			
40. DISTRIBUTION STATEMENT Unrestricted			
41. DISTRIBUTION STATEMENT Unrestricted			
42. DISTRIBUTION STATEMENT Unrestricted			
43. DISTRIBUTION STATEMENT Unrestricted			
44. DISTRIBUTION STATEMENT Unrestricted			
45. DISTRIBUTION STATEMENT Unrestricted			
46. DISTRIBUTION STATEMENT Unrestricted			
47. DISTRIBUTION STATEMENT Unrestricted			
48. DISTRIBUTION STATEMENT Unrestricted			
49. DISTRIBUTION STATEMENT Unrestricted			
50. DISTRIBUTION STATEMENT Unrestricted			
51. DISTRIBUTION STATEMENT Unrestricted			
52. DISTRIBUTION STATEMENT Unrestricted			
53. DISTRIBUTION STATEMENT Unrestricted			
54. DISTRIBUTION STATEMENT Unrestricted			
55. DISTRIBUTION STATEMENT Unrestricted			
56. DISTRIBUTION STATEMENT Unrestricted			
57. DISTRIBUTION STATEMENT Unrestricted			
58. DISTRIBUTION STATEMENT Unrestricted			
59. DISTRIBUTION STATEMENT Unrestricted			
60. DISTRIBUTION STATEMENT Unrestricted			
61. DISTRIBUTION STATEMENT Unrestricted			
62. DISTRIBUTION STATEMENT Unrestricted			
63. DISTRIBUTION STATEMENT Unrestricted			
64. DISTRIBUTION STATEMENT Unrestricted			
65. DISTRIBUTION STATEMENT Unrestricted			
66. DISTRIBUTION STATEMENT Unrestricted			
67. DISTRIBUTION STATEMENT Unrestricted			
68. DISTRIBUTION STATEMENT Unrestricted			
69. DISTRIBUTION STATEMENT Unrestricted			
70. DISTRIBUTION STATEMENT Unrestricted			
71. DISTRIBUTION STATEMENT Unrestricted			
72. DISTRIBUTION STATEMENT Unrestricted			
73. DISTRIBUTION STATEMENT Unrestricted			
74. DISTRIBUTION STATEMENT Unrestricted			
75. DISTRIBUTION STATEMENT Unrestricted			
76. DISTRIBUTION STATEMENT Unrestricted			
77. DISTRIBUTION STATEMENT Unrestricted			
78. DISTRIBUTION STATEMENT Unrestricted			
79. DISTRIBUTION STATEMENT Unrestricted			
80. DISTRIBUTION STATEMENT Unrestricted			
81. DISTRIBUTION STATEMENT Unrestricted			
82. DISTRIBUTION STATEMENT Unrestricted			
83. DISTRIBUTION STATEMENT Unrestricted			
84. DISTRIBUTION STATEMENT Unrestricted			
85. DISTRIBUTION STATEMENT Unrestricted			
86. DISTRIBUTION STATEMENT Unrestricted			
87. DISTRIBUTION STATEMENT Unrestricted			
88. DISTRIBUTION STATEMENT Unrestricted			
89. DISTRIBUTION STATEMENT Unrestricted			
90. DISTRIBUTION STATEMENT Unrestricted			
91. DISTRIBUTION STATEMENT Unrestricted			
92. DISTRIBUTION STATEMENT Unrestricted			
93. DISTRIBUTION STATEMENT Unrestricted			
94. DISTRIBUTION STATEMENT Unrestricted			
95. DISTRIBUTION STATEMENT Unrestricted			
96. DISTRIBUTION STATEMENT Unrestricted			
97. DISTRIBUTION STATEMENT Unrestricted			
98. DISTRIBUTION STATEMENT Unrestricted			
99. DISTRIBUTION STATEMENT Unrestricted			
100. DISTRIBUTION STATEMENT Unrestricted			



UNCLASSIFIED

**Naval Research Advisory
Committee Report**



Information Technology Interoperability

November 1998

**DISTRIBUTION AUTHORIZED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS
ONLY TO PROTECT INFORMATION FROM AUTOMATIC DISSEMINATION AS OF 1 NOVEMBER
1998. FURTHER DISSEMINATION OF THIS DOCUMENT IS AUTHORIZED ONLY AS DIRECTED
BY THE NAVAL RESEARCH ADVISORY COMMITTEE.**

**OFFICE OF THE ASSISTANT SECRETARY OF THE NAVY
(RESEARCH, DEVELOPMENT AND ACQUISITION)**

Table of Contents

Report Documentation Page	i
Title Page	ii
Table of Contents	1
Executive Summary	3
Outline	7
Panel Membership	9
Briefings and Visits	11
Terms of Reference	13
Definition	15
Study Scope	17
Complexity and Focus	19
Drivers	21
Take Away	23
Baseline	25
Findings	27
Good News	35
Plans and Procedures	37
Infosystem Interoperability "Seven-Layer" Open Systems Model	51
Virtual Operations Network Concept	53
Range of Solutions	59
Enabling Technologies	61
Technical Recommendations	65
Strategy and Recommendations	71
Take Away	81
Opportunity	83
Appendix A. Briefings/Panel Discussions/Video Teleconferences/ Visits	A-1
Appendix B. Terms of Reference	B-1
Appendix C. Program, Concept, and Systems Descriptions	C-1
Appendix D. Acronyms	D-1

Table of Contents

1	Report Documentation Page
4	This Page
1	Table of Contents
3	Executive Summary
7	Outline
9	Panel Membership
11	Findings and Views
13	Terms of Reference
15	Definition
17	Study Scope
19	Complexity and Focus
21	Drivers
23	Take Away
25	Baseline
27	Findings
29	Good News
37	Plans and Procedures
51	Information Interoperability "Seven-Layer" Open Systems Model
53	Virtual Operations Network Concept
59	Range of Solutions
61	Enabling Technologies
65	Technical Recommendations
71	Strategy and Recommendations
81	Take Away
83	Opportunity
	Appendix A: Briefings/and Discussions/Video Testimonials
A-1	Views
B-1	Appendix B: Terms of Reference
C-1	Appendix C: Program, Concept, and Systems Descriptions
D-1	Appendix D: Acronyms

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 partner's 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

Four 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(C⁴ISR) designate a single US authority to be proactive on interoperability issues with NATO, allied and coalition forces
 - DASN(C⁴I)/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(C⁴ISR) utilize PKI technology
 - DASN(C⁴I) adopt and enhance high assurance, programmable guard technology
 - ASD(C⁴ISR) adopt the Secret and Below Initiative (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(C⁴ISR)/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!

- **Administrative Items**
- **Background**
- **Interoperability Obstacles**
- **Plans/Procedures**
- **Existing and Near-term Technologies**
- **Strategy/Recommendations**

The brief contains the following key sections:

- **Administrative Items** contains Panel membership, briefings, visits, and the Terms of Reference (TOR).
- **Background** which includes definition, study scope, drivers, take aways and study baseline.
- **Interoperability Obstacles** includes both policy and technical obstacles as well as a brief description of existing policies and plans.
- **Plans/Procedures** describes existing organization limits, plans, procedures, standards and recommendations to improve.
- **Existing and Near-Term Technologies** – The interoperability VON is described as well as required enabling technologies and technology recommendations.
- **Strategy/Recommendations** for the DON are described along with the opportunities at hand.

Outline

- Administrative Items
- Background
- Interoperability Obstacles
- Plans/Procedures
- Existing and Near-Term Technologies
- Strategy/Recommendations

The brief contains the following key sections:

- Administrative Items contains Panel membership, background, vision, and the Terms of Reference (TOR).
- Background which includes definition, study scope, drivers, take aways and study baseline.
- Interoperability Obstacles includes both policy and technical obstacles as well as a brief description of existing policies and plans.
- Plans/Procedures describes existing organization limits, plans, procedures, standards and recommendations to improve.
- Existing and Near-Term Technologies - The interoperability VON is described as well as required enabling technologies and technology recommendations.
- Strategy/Recommendations for the DON are described along with the opportunities at hand.



Panel Membership

Information
Technology
Interoperability

<u>Chairperson</u> Ms. Katherine C. Hegmann	Senior Vice President	Lockheed Martin
<u>Vice Chairperson</u> Mr. Tom Brancati	Chairman and CEO	CPFG Inc.
<u>Panel Members</u> Dr. L. Raymond "Ray" Hettche VADM J.M. "Mike" McConnell, USN (Ret.) RADM Scott L. Sears, USN (Ret.) Mr. James M. Sinnett LtGen Keith A. Smith, USMC (Ret.) Dr. Robert C. Spindel Dr. George E. Webber RADM Richard A. Wilson, USN (Ret.) Mr. George B. Windsor	Director, Applied Research Laboratory Vice President Vice President Vice President Private Consultant Director, Applied Physics Laboratory Vice President Director, Joint Military Programs Senior Principle Engineer	Pennsylvania State University Booz Allen and Hamilton, Inc. General Dynamics The Boeing Company University of Washington Wang Government Services, Inc. SPARTA, Inc. The Boeing Company
<u>Sponsor</u> VADM Arthur K. Cebrowski, USN	Director, Space, Information Warfare, Command and Control	Office of CNO (N6)
<u>UK Representatives</u> RADM Richard T.R. Phillips, CB, RN CDR Gordon R. Graham, RN	Asst Chief of Defence Staff OR(Sea) Staff Weapon Engineer Officer	Ministry of Defence British Defence Staff, British Embassy
<u>Executive Secretary</u> LCDR David Jakubek, USN	Program Officer, Command, Control and Computer Technology	Office of Naval Research

Panel Membership

In order to credibly address the broad range of issues associated with IT interoperability, a panel of five NRAC members was augmented with experts from industry, academia and government, including three retired Navy Flag officers, a retired Marine Corps General officer, a British Navy Flag officer and a British Commander, with all having extensive IT backgrounds. Specific areas of panel expertise include system architecture, communications, networking, security technology, antenna technology, and operational experience.

The sponsor of the study was Vice Admiral Arthur K. Cebrowski, Director, Space, Information Warfare, Command and Control (N6), OPNAV.

The NRAC IT Interoperability Panel was chaired by Ms. Katherine C. Hegmann. Mr. Thomas A. Brancati served as the Vice Chairman, and Lieutenant Commander David Jakubek, Program Officer, Command, Control and Computer Technology, Office of Naval Research, served as the Executive Secretary.



Briefings/Visits

Information
Technology
Interoperability

<u>Date</u>	<u>Briefing/Visit</u>	<u>Location</u>
5/18/98	Network Centric Warfare/IT-21 ONR/DARPA Technologies Sixth Fleet Operations/Issues CNA Study on USN C4I Interoperability	Arlington, Virginia
5/19/98 - 5/22/98	CINCUSNAVEUR UK Ministry of Defence NAVCENT DERA SHAPE	London, England Brussels, Belgium
6/9/98	CINCLANTFLT, CINCPACFLT, CINCUSACOM/SACLANT SR-98 Overview C4I Overview Operational Requirements/Intelligence Overview	Norfolk, Virginia
6/10/98	Industry Briefs	Arlington, Virginia
7/7/98 - 7/8/98	VTC with Commander SPAWAR Systems Command NRL Technology Initiatives Joint Continuous Strike Environment Link 16 ACTD	Manassas, Virginia
7/13/98 - 7/24/98	I MEF, G6, Camp Pendleton QUALCOMM Navy Center For Tactical System Interoperability PEO Space Communication Systems JWID 98	San Diego, California

Briefings/Visits

The Panel conducted several visits and received numerous briefings to get background information on the IT Interoperability issue. The Panel met with the Commander in Chief, US Naval Forces, Europe (CINCUSNAVEUR); the UK Ministry of Defence, Defence Evaluation and Research Agency (DERA); Supreme Headquarters Allied Powers Europe (SHAPE); Commander in Chief, US Atlantic Fleet (CINCLANTFLT); Commander Second Fleet; and Commander in Chief, US Atlantic Command (CINCUSACOM)/Supreme Allied Commander Atlantic (SACLANT). The results of operational exercises and NATO/allied operations were reviewed with the Panel.

Video Teleconferences (VTC) and telephone conferences were conducted with US Naval Forces, US Central Command (NAVCENT) and Commander in Chief, US Pacific Fleet (CINCPACFLT) to gain insight from operational exercises. Technology briefings were received from the following organizations: OPNAV N6, SPAWAR, DISA, National Security Agency (NSA), Office of Naval Research (ONR), Defense Advanced Research Projects Agency (DARPA), Center for Naval Analyses (CNA), Naval Research Laboratory (NRL), Advanced Concept Technology Demonstration (ACTD) Program Managers, and several industry representatives.

A VTC was conducted with the Commander SPAWAR to discuss current acquisition strategies for IT Interoperability.

A detailed listing of the briefings and visits is contained in Appendix A.

Location	Subject	Date
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01
Naval Air Station, Jacksonville, FL	Naval Air Station Jacksonville Briefing	11/11/01

Appendix A

The Panel conducted several visits and received numerous briefings to get background information on the IT interoperability issue. The Panel met with the Commander in Chief, US Naval Forces Europe (CINUSNAVEUR); the UK Ministry of Defence, Defence Evaluation and Research Agency (DERA); Supreme Headquarters Allied Powers Europe (SHAPE); Commander in Chief, US Atlantic Fleet (CINCLANTFLT); Commander Second Fleet; and Commander in Chief, US Atlantic Command (CINUSACOM). The results of operational exercises and NATO/Allied operations were reviewed with the Panel.

Video Teleconferences (VTC) and telephone conferences were conducted with US Naval Forces, US Central Command (USCENTCOM) and Commander in Chief, US Pacific Fleet (CINCPACFLT) to gain insight into operational exercises. Technology briefings were received from the following organizations: SPAWAR, NSA, SPAWAR, DIA, National Security Agency (NSA), Office of Naval Research (ONR), Defense Advanced Research Projects Agency (DARPA), Center for Naval Analysis (CNA), Naval Research Laboratory (NRL), Advanced Concept Technology Demonstration (ACTD) Program Managers, and several industry representatives.

Terms Of Reference

**Information
Technology
Interoperability**

Objective

- **Assess technology and interoperability implications associated with NATO and coalition forces**

Specific tasking

- **Identify interoperability obstacles relative to joint, NATO, and coalition forces**
- **Evaluate current and envisioned plans/procedures to mitigate adverse effects**
- **Provide assessment of existing and near-term technology**
- **Recommend DoN strategy to achieve/obtain levels of interoperability in support of naval mission**

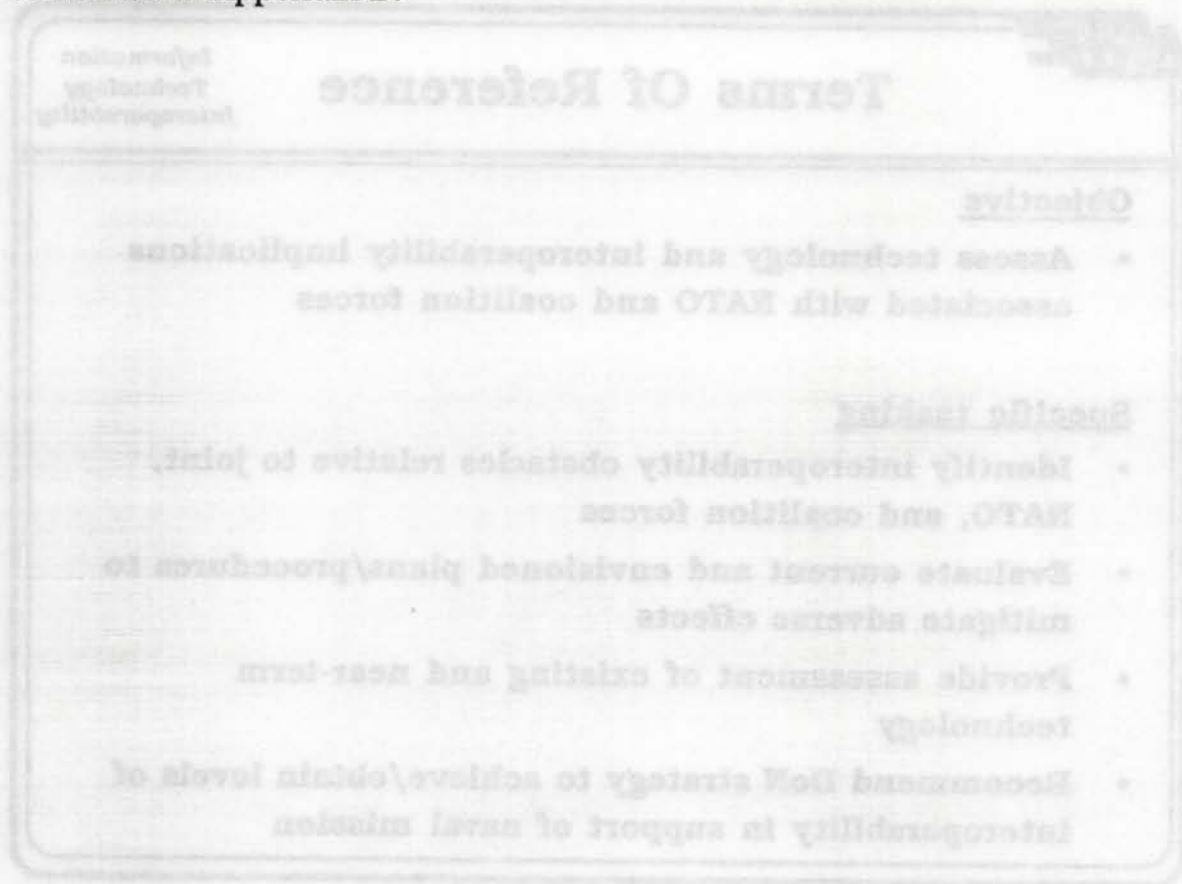
Terms of Reference

In the course of NATO, allied and coalition operations and exercises in Europe, Admiral Lopez, CINCUSNAVEUR, finds increasing problems in maintaining effective communications with non-US forces. Additionally, Admiral Lopez advises that military leaders of NATO and allied countries are concerned that the US Navy's rapid incorporation of new IT technology will "leave them behind, unable to catch-up." This concern is exacerbated by the rapid advance of the Information Technology for the 21st Century (IT-21) Program.

Admiral Clemens, CINCPACFLT, the driving force behind IT-21, believes the way to ensure effective communications with NATO, allies and coalition partners in the future is to move to COTS products as the means to "standardize" and to lower costs. Admiral Clemens' reasoning is that both standardization and lower costs will reduce the barriers to entry which will benefit both the DON and NATO, allied and coalition partners of the future.

In March, 1998, Admiral Lopez requested that NRAC assess IT Interoperability with NATO and coalition forces and propose a strategy and recommendations on how to ensure that appropriate levels of communications can be maintained with our partners as the US Navy

embraces rapidly changing IT technology. The complete TOR for the study is contained in Appendix B.



Terms of Reference

In the course of NATO, allied and coalition operations and exercises in Europe, Admiral Lopez, CINCPACFLT, finds increasing problems in maintaining effective communications with non-US forces. Additionally, Admiral Lopez advises that military leaders of NATO and allied countries are concerned that the US Navy's rapid incorporation of new IT technology will "leave them behind, unable to catch-up". This concern is exacerbated by the rapid advance of the Information Technology for the 21st Century (IT-21) Program.

Admiral Chinn, CINCPACFLT, the driving force behind IT-21, believes the way to ensure effective communications with NATO, allies and coalition partners in the future is to move to COTS products as the means to "standardize" and to lower costs. Admiral Chinn's reasoning is that both standardization and lower costs will reduce the barriers to entry which will benefit both the DON and NATO, allied and coalition partners of the future.

In March, 1998, Admiral Lopez requested that WRAC assess IT interoperability with NATO and coalition forces and propose a strategy and recommendations on how to ensure that appropriate levels of communications can be maintained with our partners as the US Navy

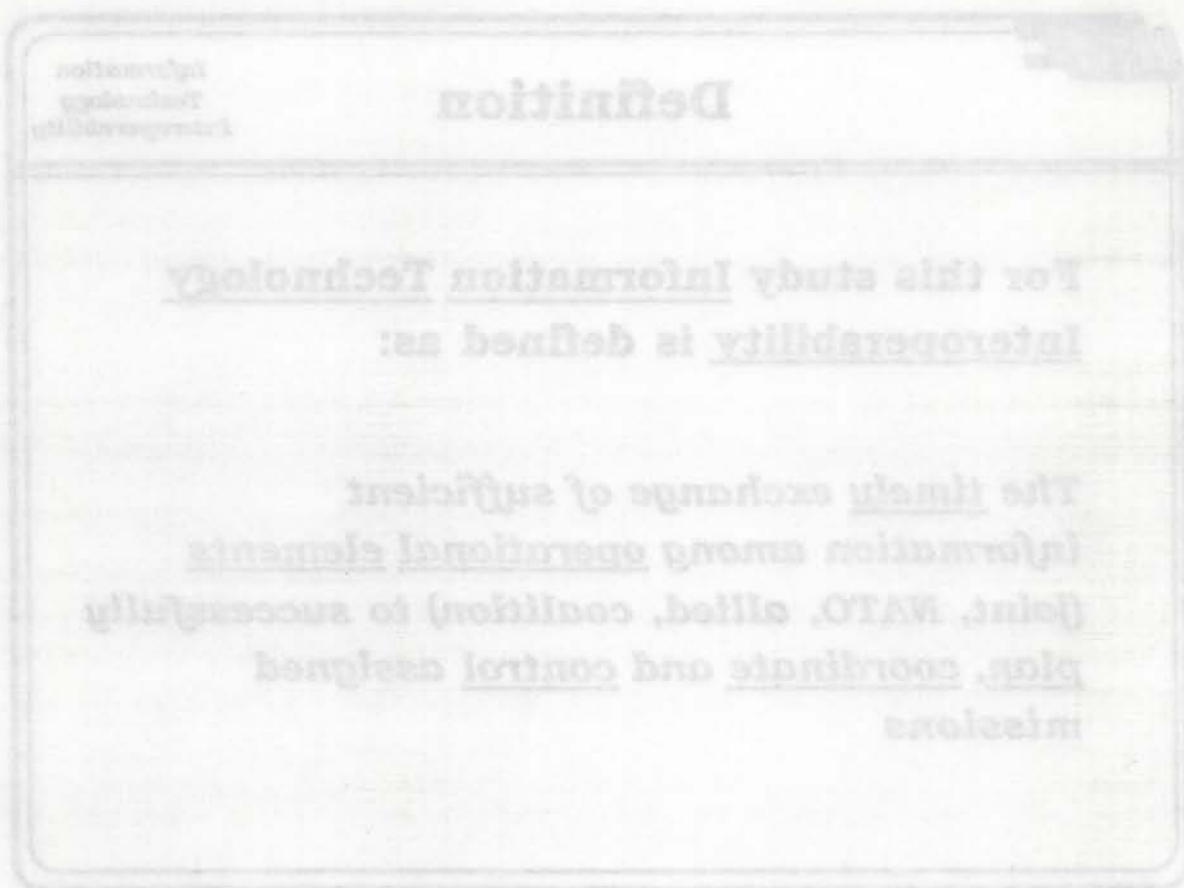
For this study Information Technology Interoperability is defined as:

The timely exchange of sufficient information among operational elements (joint, NATO, allied, coalition) to successfully plan, coordinate and control assigned missions

Definition

While official definitions are found for such terms as interoperability, command, control, and communications, the Panel was unable to find a suitable definition for "Information Technology Interoperability." Therefore, the Panel agreed on the following definition:

The timely exchange of sufficient information among operational elements (joint, NATO, allied, coalition) to successfully plan, coordinate and control assigned missions.

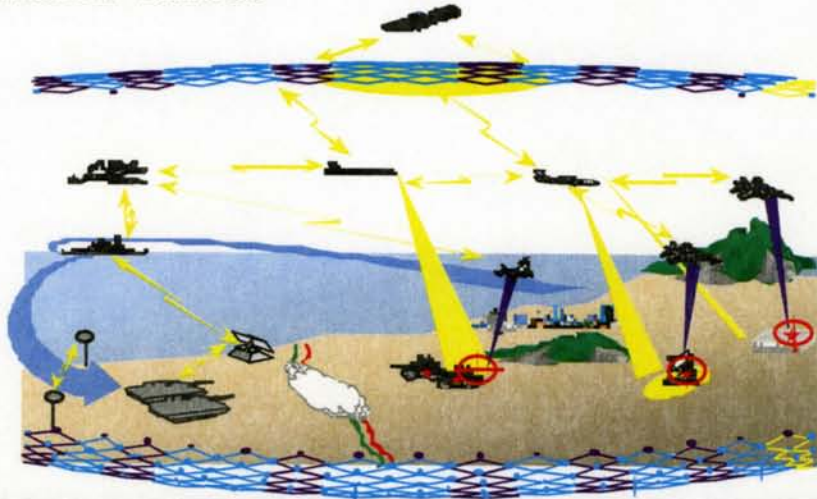


Definition

While official definitions are found for such terms as interoperability, command, control, and communications, the Panel was unable to find a suitable definition for "Information Technology Interoperability." Therefore, the Panel agreed on the following definition:

The timely exchange of sufficient information among operational elements (Joint, NATO, allied, coalition) to successfully plan, coordinate and control assigned missions.

Assess interoperability implications relative to US Naval operations with NATO, Allied and coalition forces



Study Scope

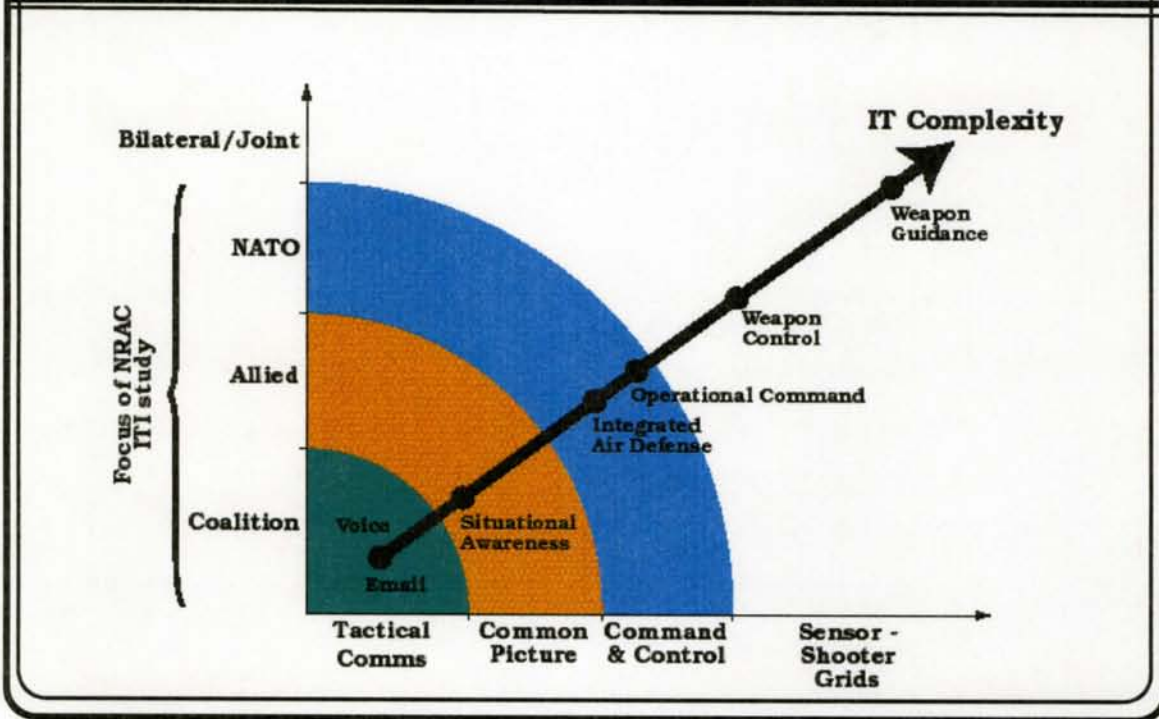
Consistent with Admiral Lopez' concern, the study addresses US Naval operations with NATO, allied and coalition forces. There are significant efforts underway addressing DON and joint forces IT interoperability issues, but relatively little is being done with NATO, Allied and coalition forces.



Consistent with Admiral Lopez' concern, the study addresses US Naval operations with NATO, Allied and coalition forces. There are significant efforts underway addressing DON and joint forces IT interoperability issues, but relatively little is being done with NATO, Allied and coalition forces.

Complexity and Focus

Information
Technology
Interoperability

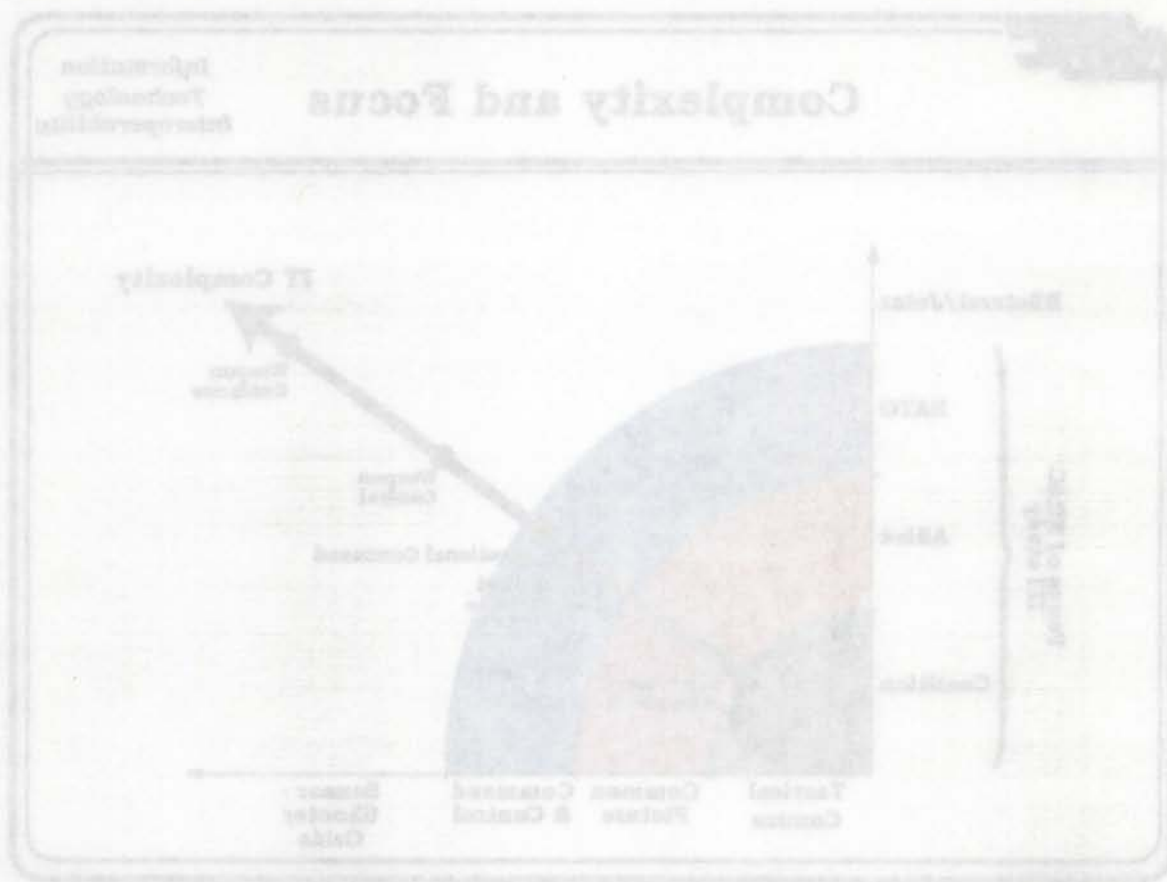


Complexity and Focus

The above chart expands and further explains the Panel's focus. It shows "IT Complexity" compared to functionality, and illustrates while minimum effective interoperability may be required by coalition partners, maximum interoperability is required with NATO partners. The Panel observed that complexity increased proportionally with the technical sophistication of our partners. It was also noted that the more technically sophisticated the partner, the more complex the exchange of functional requirements. The Panel concluded that Operational Command and Integrated Air Defense functions are the most complex exchanges between the US forces and the forces within the focus of the study (NATO, Allied and coalition). The study addresses the issues shown in the shaded portion of the chart.

The above chart expands and further explains the Panel's focus. It shows "IT Complexity" compared to functionality, and illustrates with minimum effective interoperability may be required by coalition partners. The Panel observed that complexity increased proportionally with the technical sophistication of our partners. It was also noted that the more technically sophisticated the partner, the more complex the exchange of functional requirements. The Panel concluded that Operational Command and Integrated Air Defense functions are the most complex exchanges between the US forces and the forces within the focus of the study (NATO, Allied and coalition). The study addresses the issues shown in the shaded portion of the chart.

Complexity and Focus



Drivers

Information
Technology
Interoperability

- **US will continue to push technology solutions**
- **US Forces need interoperable partners**
- **Each partner's classified information assets must be protected**
- **Network Centric Warfare places additional demands on interoperability**
- **Coalition partners determined *ad hoc***
- **Requirements for interoperability will vary**

Drivers

The US is the global leader in the IT industry, now the largest industry in the world. IT has increased productivity and fueled economic growth for over a decade as new products and services have been developed. Some argue that society is being transformed by IT especially with access to the Internet, which connects citizens and markets around the globe. There are a number of key points that become drivers for the study. It was recognized that the DON will continue to push new technology solutions toward improving C⁴ISR capabilities to make our forces more efficient and effective. In fact, the Joint Chiefs of Staff publication "Joint Vision 2010" declares that the US Military of the future will rely on having "Information Superiority" driven by IT.

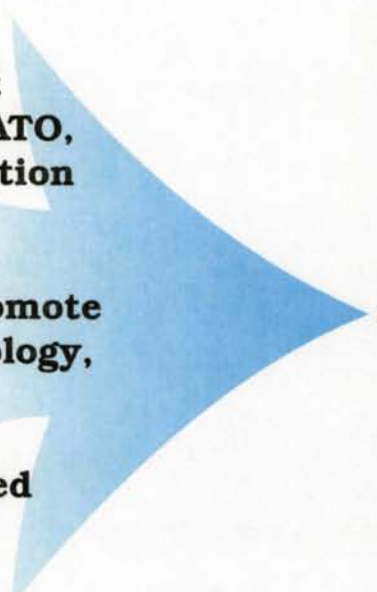
In order to harness the power of the revolution in IT, there is a need for appropriate protection of classified information to inform and protect US, NATO, allied and coalition partners. The US must balance protection of allied and coalition information, which is shared, against US only information, which cannot be shared. The move to achieve "information superiority" through such initiatives as "Network Centric Warfare," while providing adequate protection of classified data, puts increased stress on NATO, allied and coalition force interoperability requirements. Demands for volume and timeliness will continue to increase.

Unlike the long established structure of NATO, which has been ratified through treaty, coalition partners are often determined ad hoc depending on the requirements of the situation. Two examples are: Syrian forces joining in the coalition to force the Iraqis out of Kuwait in 1991; and more recently, the wide variety of UN partners in the Bosnian crisis in the former Yugoslavia. It is US policy not to serve as the world's policeman. However, with the strongest economy and the strongest military in the world, we inevitably will be drawn into regional conflicts to preserve world peace. Accordingly, the US policy of "Global Engagement" seeks to ensure that we have allies, partners and global support when and if US Forces are committed. IT interoperability with these allies and partners will significantly enhance the effectiveness of carrying out assigned missions.

The final driver is recognition of the fact that military capabilities and IT interoperability capabilities of allies and potential coalition partners vary widely. UK Forces are more technologically advanced than the forces of Greece, Bulgaria or Thailand. These wide variances are the major factor influencing the conclusions and recommendations of the Panel. We have to accommodate a wide spectrum of interoperability requirements.

Take Away

Information
Technology
Interoperability

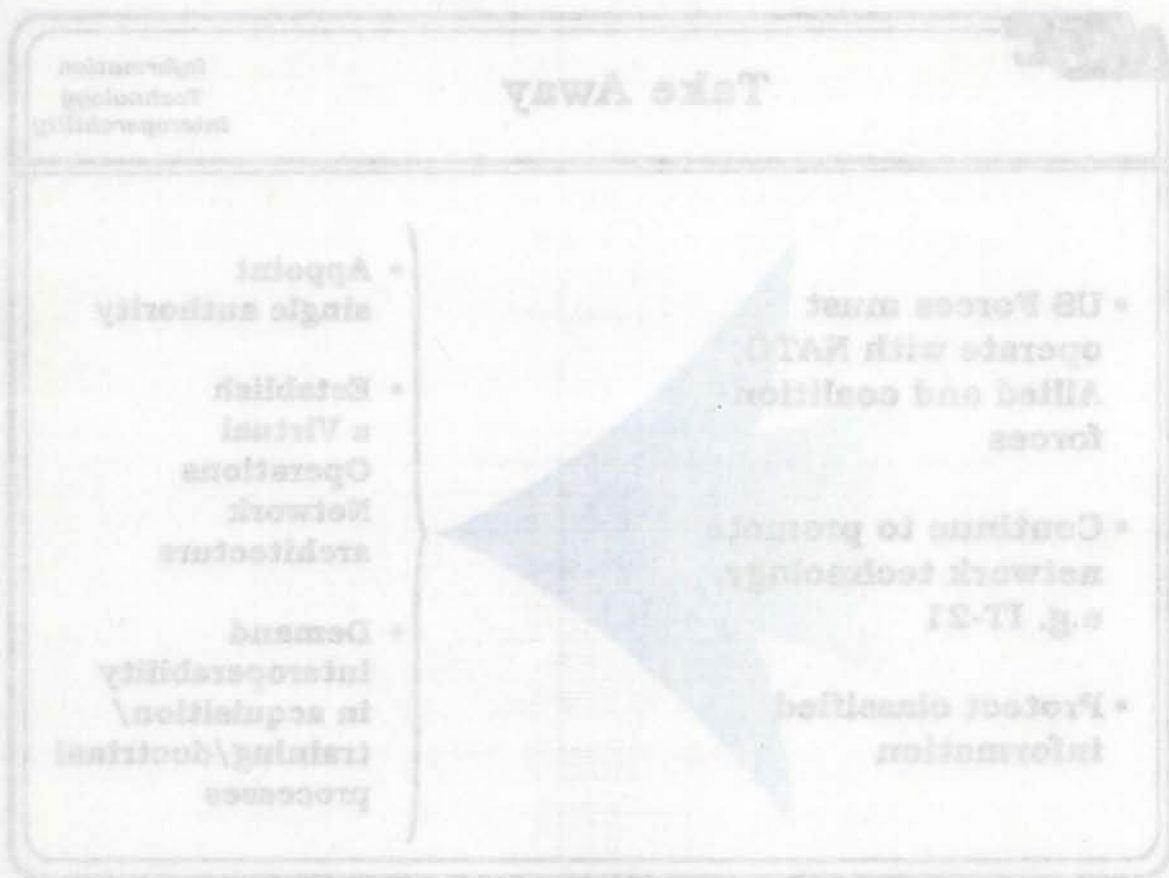
- 
- **US Forces must operate with NATO, Allied and coalition forces**
 - **Continue to promote network technology, e.g. IT-21**
 - **Protect classified information**
- **Appoint single authority**
 - **Establish a Virtual Operations Network architecture**
 - **Demand interoperability in acquisition/training/doctrinal processes**

Take Away

The US Navy and US Marine Corps need to focus their efforts to increase interoperability with NATO, Allied and coalition forces. In order to address broad IT interoperability requirements and solutions, the DON should recommend that the Secretary of Defense (SECDEF) and Chairman of the Joint Chiefs of Staff (CJCS) designate a single US authority for interoperability with NATO, Allied and coalition forces. This authority should coordinate across joint, NATO, Allied and potential coalition partners. An authority should also be established within DON to address DON interoperability issues.

To achieve a minimum capability to communicate with all our partners, creation of a VON is recommended. The DON should invest in enabling technologies to achieve VON capabilities. Additionally, the DON should establish minimum equipment sets to provide to coalition partners who lack capability.

Finally, DON should consider modifications in its acquisition process to demand interoperability requirements. Currently the acquisition system and processes are incentivized in areas other than achieving IT interoperability.



Take Away

The US Navy and US Marine Corps need to focus their efforts to increase interoperability with NATO, Allied and coalition forces. In order to address these IT interoperability requirements and solutions, the DON should recommend that the Secretary of Defense (SECDEF) and Chairman of the Joint Chiefs of Staff (CJCS) designate a single US authority for interoperability with NATO, Allied and coalition forces. This authority should coordinate across joint, NATO, Allied and potential coalition partners. An authority should also be established within DON to address DON interoperability issues.

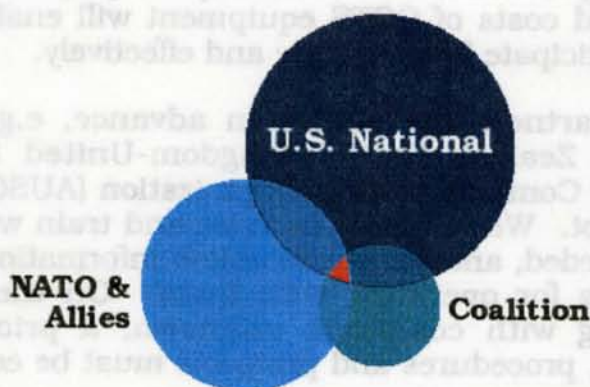
To achieve a minimum capability to communicate with all our partners, creation of a VON is recommended. The DON should invest in enabling technologies to achieve VON capabilities. Additionally, the DON should establish minimum equipment sets to provide to coalition partners who lack capability.

Finally, DON should consider modifications in its acquisition process to demand interoperability requirements. Currently the acquisition system and processes are incentivized in areas other than achieving IT interoperability.

Baseline

Information
Technology
Interoperability

- Coalition partners not known *a priori*
- Information infrastructure is unequal
- Information interoperability is minimal



Baseline

Unequal information infrastructure levels hamper US operations with Allied and coalition forces. Inequalities exist in access to the basic required hardware and software equipment, in expertise in its use, in readiness and training of information forces, and in national commitments to successfully achieving effective joint operations. The US has the largest investment and dependence on sophisticated information technologies for the conduct of the full spectrum of naval warfare, and is committed to a rapid pace of advance. Most Allied nations, although equally technically proficient, have not invested in either a commercial or military information infrastructure to the extent of the US, and therefore possess a range of capability, from near equality on the part of the UK, France, Canada and Australia, for example, to equal skill, but less investment in the required hardware, on the part of Spain, Greece and Italy. Coalition partners generally are less capable. Partners for Peace (PfP) nations are at a lower baseline still; many do not have access to modern COTS technology due to budget limits or export restrictions.

Such disparate capability is a major obstacle to effective joint operations. Something as routine and simple as e-mail may not be available to all parties, and sometimes, even if it is, different formatting and transfer protocols forestall effective communications. More sophisticated and

bandwidth intensive functions, such as video teleconferencing, which is rapidly becoming the US de facto method for high-level command communications, may be completely unavailable even to the our most sophisticated and technically advanced allies.

The perception of many US Allies is that the situation is getting rapidly worse because of the speed with which the US is moving towards implementing the full spectrum of Network Centric Warfare, and the incorporation of IT-21 enabling technology into Naval forces. There is a feeling that the US is not including our Allied partners in the critical decisions required to ensure a continued capability to operate jointly with them. The US position is that IT-21, COTS-based information technologies with standard network protocols, will ultimately simplify interoperability, and further, the reduced costs of COTS equipment will enable Allied and coalition partners to participate fully, equally and effectively.

Whereas Allied partners are known in advance, e.g., NATO and Australia-Canada-New Zealand-United Kingdom-United States Naval Command, Control, and Communications Organization (AUSCANNZUKUS), coalition partners are not. We routinely exercise and train with our Allies, albeit not as often as needed, and we can establish information interchange procedures and policies for operating with them. On the other hand, training and exercising with coalitions unknown, a priori, is clearly impossible; and policies, procedures and protocols must be established on-the-spot.

Findings

Information
Technology
Interoperability

Policy Obstacles

- **National interests**
 - **Security/releasability different for various NATO, Allied and coalition partners**
 - **Each country has its own C4I structure**
 - **Bilateral agreements**
- **No single well-defined interoperability authority**
- **Systems not designed with interoperability in mind**
- **Inadequate emphasis on interoperability during training and exercises**

Findings (Policy Obstacles)

Many of the obstacles that mitigate against achieving seamless interoperability with Allied and coalition forces are rooted in policy and management procedures.

The single most important issue is the need to protect national interests, assets and resources. Each nation has its own unique security structure and releasability guidelines. Present US policy, for example, restricts access to the SECRET Internet Protocol Router Network (SIPRNET), the backbone of our military information highway. While Allied and coalition partners may be given distilled, or need-to-know intelligence, they cannot access the full spectrum of information available. Because the release of SIPRNET information depends on manual intervention, which is a slow and labor intensive process, the necessary information is often unavailable in a timely manner. Bilateral agreements between various partners exacerbate the problem.

The most commonly cited obstacle by nearly all "users" interviewed was providing timely, secure information exchange between participants on a "need-to-know" basis. This included the ability to provide controlled access to required information which is "releasable" but which may reside in classified national systems (i.e., SIPRNET). NATO "users" consistently cited

lack of availability of interoperable cryptography and SIPRNET access as significant obstacles.

Military and political goals may have different levels of need for interoperability. Military leadership within the DON believe that Naval forces must be prepared to win the war with or without partners or interoperability, whereas our foreign policy of engagement is enhanced by interoperability and shared responsibilities.

Further, each nation has its own C⁴I structure, using different methods of C², different procedures, different data structures, interfaces and equipment. Each has a different procurement system; some not as rapid as the US, and some, like NATO, particularly cumbersome and unwieldy. In addition, NATO maintains an equipment pool to be assigned as needed, rather than a dollar pool to buy the latest equipment. As a result, in the especially rapidly advancing realm of information technologies, NATO equipment languishes on the shelf, quickly becoming obsolete. With respect to almost all of these issues, most Allies feel that, in general, the US DON attitude is to expect them to do things as we do, use what we use, and buy what we buy. In some cases they are willing to have the US set standards; in others there is a feeling of resentment that mitigates against cooperation. In the case of hardware and software the situation is particularly difficult because many nations see this as an opportunity to develop or enhance indigenous industries.

There are a plethora of agencies, offices, commands and other entities charged with managing the technical aspects of IT interoperability, but there are no well-defined interoperability authorities, either nationally or internationally. As a result, there are major incompatibilities between contemporaneous equipment and the interface of new equipment with legacy systems is unsatisfactory. The latter was identified by SECOND Fleet as their single most important problem.

Systems, as well as people, must train and exercise together to achieve the level of interoperability desired to successfully execute military missions, ie., "We fight as we train." While there are a continuing series of exercises with NATO and other Allied forces, and a lesser number with various possible coalition partners, the number that emphasize IT interoperability is insufficient. They are too infrequent to test solutions to "previously identified problems," or to develop a sense of corporate memory.

An important management issue is the status within the Naval community of information technologists, those charged with information warfare, and with IT interoperability. Well-defined career paths do not yet exist, and those that pursue careers in this direction have not yet achieved "Information Warrior" status.

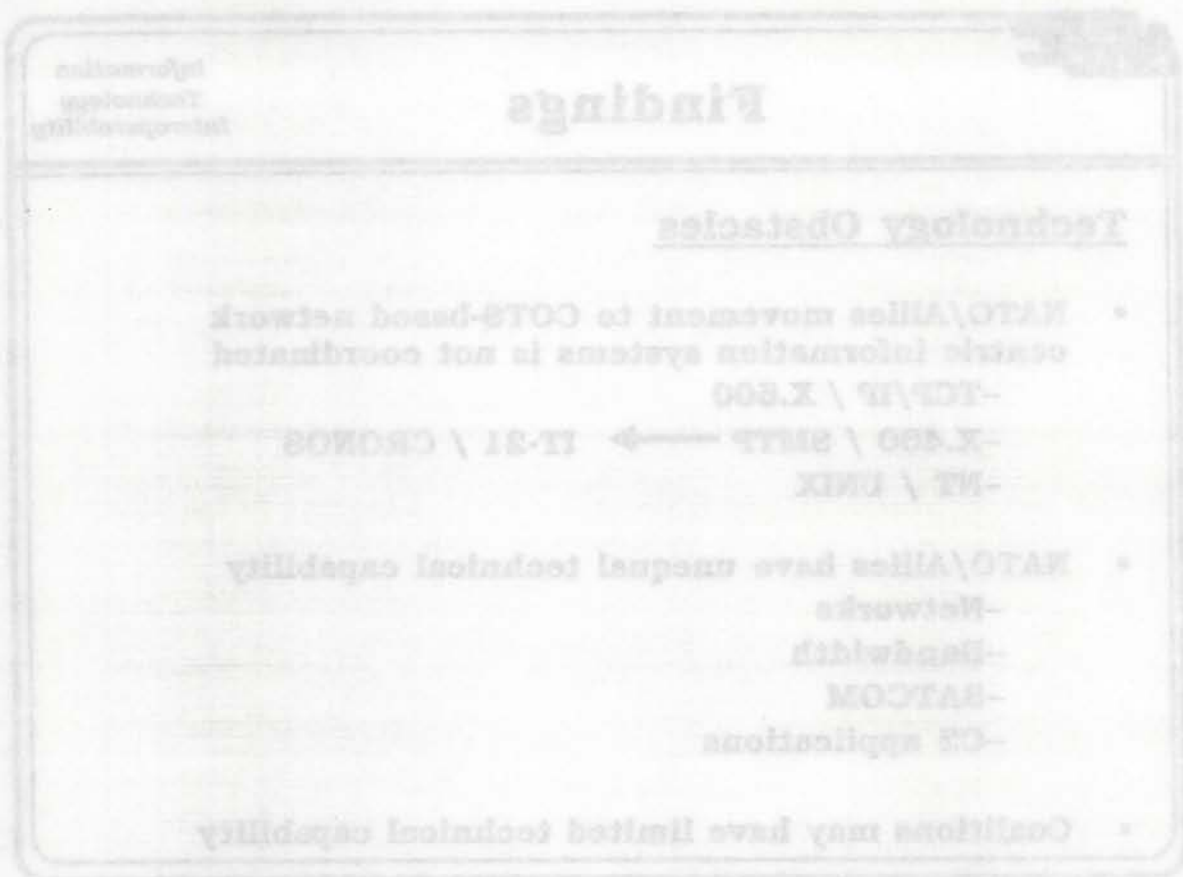
Technology Obstacles

- **NATO/Allies movement to COTS-based network centric information systems is not coordinated**
 - TCP/IP / X.500
 - X.400 / SMTP → IT-21 / CRONOS
 - NT / UNIX
- **NATO/Allies have unequal technical capability**
 - Networks
 - Bandwidth
 - SATCOM
 - C2 applications
- **Coalitions may have limited technical capability**

Findings (Technology Obstacles)

Information services required for planning and controlling NATO, Allied and coalition operations are becoming increasingly network oriented in the sense of COTS protocols and services [(TCP/IP), Industry E-mail Standard (X.400), Industry Directory Standard (X.500), Simple Mail Transfer Protocol (SMTP), Work/Station Operating System (UNIX)/Personal Computer Operating System (NT)]. They are also becoming increasingly bandwidth demanding.

The rapid incorporation of technologies into the US Navy and Marine Corps systems and evolving standards is resulting in a more effective force. However, interoperability difficulties stemming from equipment interface and compatibility problems are magnified in operations with NATO, Allied and coalition partners where there is far less control over interoperability standards; where technical capabilities can be widely disparate; and where information security and releasability is a major issue.



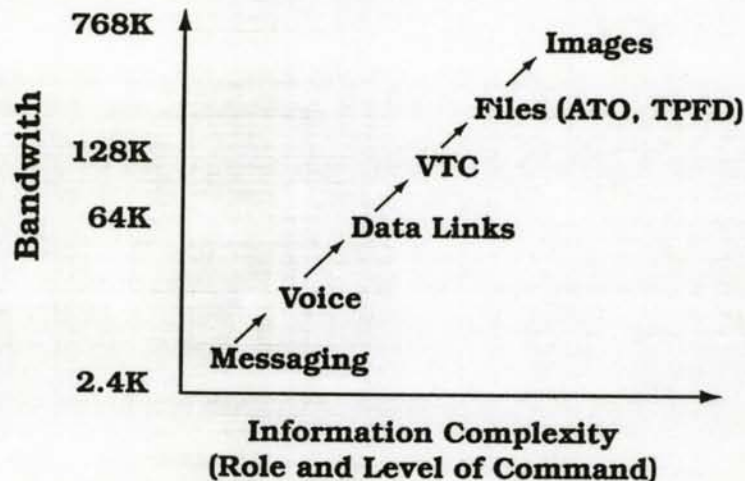
Findings (Technology Obstacles)

Information services required for planning and controlling NATO, Allied and coalition operations are becoming increasingly network oriented in the sense of COTS protocols and services (TCP/IP, industry E-mail Standard (X.400), industry Directory Standard (X.500), Simple Mail Transfer Protocol (SMTP), Work/Station Operating System (UNIX)/Personal Computer Operating System (NT)). They are also becoming increasingly bandwidth demanding.

The rapid incorporation of technologies into the US Navy and Marine Corps systems and evolving standards is resulting in a more effective force. However, interoperability difficulties stemming from equipment interface and compatibility problems are magnified in operations with NATO, Allied and coalition partners where there is far less control over interoperability standards; where technical capabilities can be widely disparate; and where information security and releasability is a major issue.

Technology Obstacles

- Bandwidth required is a function of assigned role



Findings (Technology Obstacles)

The primary information services required for force coordination and control are illustrated in this chart, together with a rough indication of bandwidth requirements for each. Of course, depending upon their role in the mission, not all participants require all services. Compatible bandwidth required is determined by the role and level of command of the participant.

The technical demands on interoperability range from simple messaging and voice communications which do not tax available bandwidth (although even here there are coalition partners who do not possess the technical capability to participate), to large database and file transfers, such as Air Tasking Orders (ATO's) and images, which are bandwidth intensive.



Findings (Technology Obstacles)

The primary information services required for force coordination and control are illustrated in this chart, together with a rough indication of bandwidth requirements for each. Of course, depending upon their role in the mission, not all participants require all services. Compatible bandwidth required is determined by the role and level of command of the participant.

The technical demands on interoperability range from simple messaging and voice communications which do not tax available bandwidth (although even here there are coalition partners who do not possess the technical capability to participate), to large databases and file transfers, such as Air Tasking Orders (ATO's) and images, which are bandwidth intensive.

Findings

Information
Technology
Interoperability

Technology Obstacles

- **"Afloat" force projection requires interoperative HF & SATCOM with common frequency allocation**
 - **Low profile antennas**
 - **SATCOM vulnerabilities**
 - **Bandwidth and information security**
- **Limitations to interoperability**
 - **Security and releasability control**
 - **Application standards for information exchange**
 - **Technology for automatic voice/text/message format translation**

Findings (Technology Obstacles)

Available land-based common user networks, such as unclassified but sensitive (N-level) Internet Protocol Router Network (NIPRNET), Crisis Response Operations in NATO Open System (CRONOS) and others, are generally capable of providing these services and bandwidths as required. However, mobile naval "afloat" operations present a unique problem which has led to a dependence on SATCOM as a necessary infrastructure element to support information exchange. Current UHF SATCOM capabilities do not provide adequate bandwidth to support full services. In addition, most UHF SATCOM communications are strictly circuit oriented and not easily integrated as an element of a TCP/IP network infrastructure. New operations concepts, which combine bandwidth-enhanced UHF SATCOM capability with the large downlink bandwidth capability of the GBS could provide enhanced information interoperability.

Other SATCOM-related technical issues included the lack of availability of standardized SATCOM terminal equipment for Allied/coalition participants, as well as availability of common frequency allocations across nations. A serious issue also was identified relating to the physical size and radar cross-section of SATCOM antennas (particularly Super High Frequency (SHF)) which limits utilization on ships where most space is

limited and cross-section is critical. SATCOM is also subject to denial by jamming, and is vulnerable to user location and identification.

As a final technical issue, we found that higher level C² applications, such as some Global Command and Control System (GCCS) applications and equivalent partner applications, often utilize different data structures and formats which make interoperability difficult. This was found to include such basic things as geolocation reference formats. Since it is unlikely that international standardization will be achieved for all such items, it is probably more fruitful to provide software based data format translation tools for critical applications that require interoperability. Such tools might be akin to the file translation tools and related "middleware" utilities commonly used in commercial word processing and spreadsheet applications for interoperating between different vendor products.



- **Use of COTS-based equipment and open systems architectures significantly improve cost/performance ratio**
 - **Lowers barrier to entry**
- **Technology invention not required**
- **Policies and procedures exist**
- **Political imperative to have partners**
- **Tactical imperative to interoperate**

Good News

While we note that movement to COTS-based systems and protocols is not well coordinated among our Allies, the use of such systems is a significant opportunity for maximizing flexibility, compatibility and interoperability. Open architectures, the existence of widely used standards (although they are not always common) and protocols, and the ready availability of relatively inexpensive commercial equipment ease the barriers to efficient and cost-effective allied and coalition participation.

The basic technologies to achieve high levels of interoperability exist, and the policies and procedures--within the US, at least--to insure interoperability of new and legacy systems are in place. The latter need to be implemented and fully incorporated into the acquisition process. And while there is need for further development and maturation of certain technologies, such as network security guards, for example, the basic underlying techniques exist.

One example of an international effort advancing interoperability is Communications Systems Network Interoperability (CSNI) which produced the Advanced Digital Network System (ADNS), a part of the IT-21 installation that Battle Group deployers are receiving today.

National political and military policies also support the concept of allied and coalition interoperability.

The pieces of the puzzle are all in place.

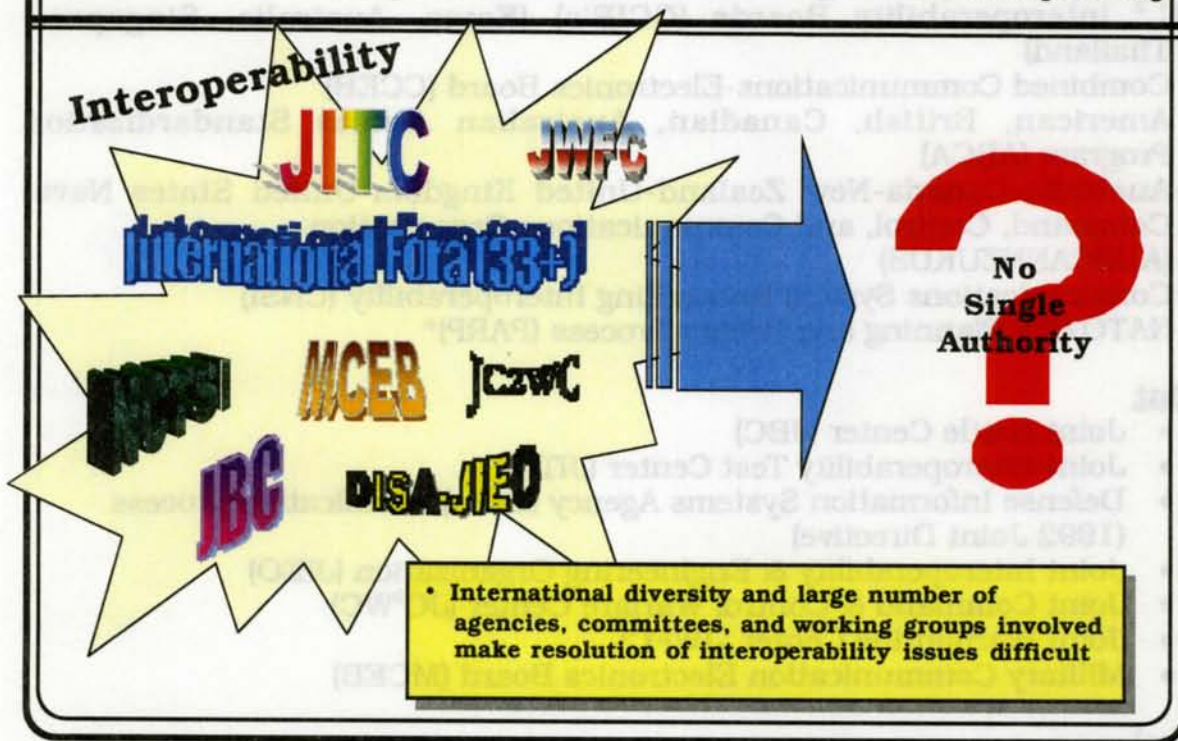
- Use of COTS-based equipment and open systems architectures significantly improve cost/performance ratio
- Lowers barrier to entry
- Technology invention not required
- Policies and procedures exist
- Political imperative to have partners
- Tactical imperative to interoperate

Good News

While we note that movement to COTS-based systems and protocols is not well coordinated among our Allies, the use of such systems is a significant opportunity for maximizing flexibility, compatibility and interoperability. Open architecture, the existence of widely used standards (although they are not always common) and protocols, and the ready availability of relatively inexpensive commercial equipment ease the barriers to efficient and cost-effective allied and coalition participation.

The basic technologies to achieve high levels of interoperability exist, and the policies and procedures—within the US, at least—to insure interoperability of new and legacy systems are in place. The latter need to be implemented and fully incorporated into the acquisition process. And while there is need for further development and maturation of certain technologies, such as network security guards, for example, the basic underlying technologies exist.

One example of an international effort advancing interoperability is Communications Systems Network Interoperability (CSNI) which produced the Advanced Digital Network System (ADNS), a part of the IT-21 installation that Battle Group deployers are receiving today.



Plans and Procedures

The Panel found it difficult to identify any single authority or well defined chain-of-command in charge of interoperability. Instead, the Panel found a wide variety of entities with separate chains of command working on various parts of the interoperability challenge. Many are not aware of the other's existence or efforts. All of these bodies appear to be well intentioned and contributing to some degree, but are missing the opportunity to leverage their effectiveness in a more coordinated and synergistic environment.

The following lists the bodies, committees, agencies, working groups, subgroups, and project groups which are to some degree involved in interoperability issues. Because of the complex nature of US involvement in a wide variety of interoperability efforts, this list should not be considered all-inclusive.

International

- Military Telecommunications and Communications and Information Systems (CIS)
- Allied Data System Interoperability Agency (ADSIA)

- Military Agency for Standardization (MAS) Service Boards (Navy, Marine Corps, Air Force, Army)
- Air Standardization Coordinating Committee (ASCC)
- Interoperability Management Board (IMB) (US, Japan)
- C² Interoperability Boards (CCIB's) (Korea, Australia, Singapore, Thailand)
- Combined Communications-Electronics Board (CCEB)
- American, British, Canadian, Australian Armies Standardization Program (ABCA)
- Australia-Canada-New Zealand-United Kingdom-United States Naval Command, Control, and Communications Organization (AUSCANNZUKUS)
- Communications System Networking Interoperability (CNSI)
- NATO/PfP Planning and Review Process (PARP)*

Joint

- Joint Battle Center (JBC)
- Joint Interoperability Test Center (JITC)
- Defense Information Systems Agency (DISA) Certification process (1992 Joint Directive)
- Joint Interoperability & Engineering Organization (JIEO)
- Joint Command & Control Warfare Center (JC²WC)
- Joint Warfighting Center (JWFC)
- Military Communication Electronics Board (MCEB)

Naval

- Navy Center for Tactical Systems Interoperability (NCTSI)
- Marine Corps Tactical Systems Support Activity (MCTSSA)

*PARP is an integral part of PfP. The participating nations identify specific forces to be provided to PfP and define their scope for improving interoperability. Partners complete a Survey of Overall PfP Interoperability. This includes forces available for operations, training and exercises within the context of PfP. The NATO staff then produces a draft Planning and Review Assessment for each partner. This includes the relevant information provided by partners, together with a set of Interoperability Objectives (IOs), which have been proposed by NATO's Military Authorities. In order for multilateral training, exercises, or operations to be successful, forces must be able to work together. The IOs are thus an important feature of PARP, which are tailored to the particular needs and requirements of each partner. The aim of the IOs is to provide each partner with a challenging but realistic set of planning goals. These goals do not create a binding commitment; but by accepting them as goals, partners commit serious efforts towards achieving them.

Current Plans

Information
Technology
Interoperability

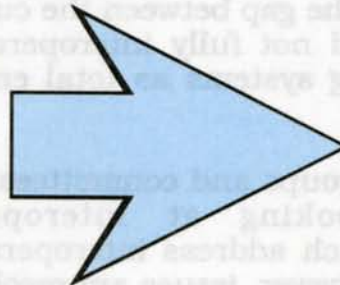
- **Information Technology Management Reform Act of 1996 establishes Chief Information Officer (CIO) concept for all government agencies**
- **DoD directives, instructions, and regulations exist, however inadequately enforced**
- **DoN CIO Strategic Plan Provides top-level guidance and direction**

CURRENT

Customers need interoperable systems

Functional organization deliver solutions through functional stovepipes

Customers get non-interoperable systems



FUTURE

Customers need interoperable systems

Functional requirements delivered through enterprise solutions

Customers provided with interoperable systems

Current Plans

The Panel observed that there are several high level plans which address the interoperability issues. On a national level, the Information Technology Management Reform Act of 1996 established the CIO concept for all government agencies. This act grants the authority and provides the mechanism for addressing interoperability problems. No known equivalent is currently in place for NATO, Allied and coalition forces.

At the DoD level, the Panel found that numerous directives, instructions and regulations which address interoperability exist. Their adequacy in terms of clarity, enforcement, and integration of effort to achieve interoperability requires improvement.

Examples of basic DoD policy and procedure documents requiring C⁴I systems certification testing for interoperability include but are not limited to:

DoD Directive 4630.5, "Compatibility, Interoperability, and Integration of C³I Systems."

DoD Instruction 4630.8, "Procedures for Compatibility, Interoperability, and Integration of C³I Systems."

DoD Regulation 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAP's) and Major Automated Information System (MAIS) Acquisition Programs.

CJCS Instruction 6212.01A, "Compatibility, Interoperability, and Integration of C⁴I Systems."

At the DON level, the CIO has developed a strategic plan which: (1) provides top-level guidance and direction for planning DON IT activity; (2) is predicated on the principles of GCCS, Global Combat Support System (GCSS) and the Defense Information Infrastructure/Common Operation Environment (DII/COE); and (3) has the objective of assisting personnel in developing IT programs that are standards compliant, meet architectural objectives and support interoperability.

The goal is to bridge the gap between the current method of delivering systems as stovepipes and not fully interoperational, to the envisioned future method of delivering systems as total enterprises and being fully interoperational.

Numerous working groups and committees exist on the NATO, allied and coalition level looking at interoperability and several directives/publications which address interoperability (i.e. Allied Tactical Publications 1 (ATP-1)). However, issues are resolved slowly. This is due to the sheer number of countries involved, the difference in systems employed and the internal policy and politics of each nation.

The DON CIO strategy needs to include emphasis on interoperability with our NATO, allied and coalition partners. Success in this area could be best achieved by appointing a deputy whose focus is on interoperability.

Standards

Information
Technology
Interoperability

- Many different standards available
- Numerous organizations working IT standards, little concurrence
- Interoperability requires compatible standards

US/Joint	NATO/Allied/Coalition	Industry
<div style="text-align: center;">← <u>Organizations</u> →</div>		
<ul style="list-style-type: none"> • DISA • MCEB • JIEO • JITC • NCTSI 	<ul style="list-style-type: none"> • 33 + International Fora 	<ul style="list-style-type: none"> • ISO
<div style="text-align: center;">← <u>Standards</u> →</div>		
<ul style="list-style-type: none"> • DII/COE • JTA • DMS Messaging (X.400/X.500) • COTS (Windows NT/UNIX) 	<ul style="list-style-type: none"> • X.400 • COTS (Windows NT/UNIX) • STANAGS 	<ul style="list-style-type: none"> • SMTP • Windows NT/UNIX • X.400 • X.500 • HTTP/HTML (WEB)

Standards

A major US goal is adoption of common or compatible standards that will ensure interoperability among NATO, allied and coalition C² Information Exchange Systems. Armed conflicts can be expected to involve the use of combined military forces. To use these forces effectively, the need exists to increase fighting capability through compatibility among the various C² information systems and interoperability at the information level. This can be done through the adoption and development of standards and systems designed to provide interoperability through the use of approved data and information exchange standards. In the combined environment, an additional advantage is the alleviation of information exchange problems associated with differing national languages and military organizational structures.

Because of a large national investment in tactical C² systems and associated experience in developing and supporting standards, the US is in the best position to play a leading role in developing and promoting allied acceptance of combined interoperability standards.

DISA has taken the lead in this area and developed an architecture/approach for building interoperable systems called the DII/

COE. DII/COE is mandated by US law and provides a foundation for building an open system while facilitating software reuse.

The optimum situation is to develop a standard which is adopted/accepted by everyone. However, in those cases where a single standard is not accepted due to political, fiscal or technical issues, translators can usually be developed which help to mitigate this problem. The goal should be to continue efforts to minimize those situations where a common standard cannot be realized.

In addition to DISA, numerous other organizations address the standards and interoperability issues. Several examples are:

Joint

- DISA
- Joint Chiefs of Staff (JCS)/J6 - (MCEB)
- Interoperability Improvement Panel (IIP)
- Interoperability Test Panel (ITP)
- JIEO
- Joint Multi-Tactical Digital Information Link (TADIL) Standards Working Group (JMTSWG)
- Configuration Control Board (CCB)
- JITC

Navy





- NCTSI
- Operations Interoperability Requirements Group (OIRG)
- Technical Interoperability Standards Group (TISG)
- Implementation Action Council for C² Systems

NATO

- NATO C³ Board/Information Systems Sub-Committee
- Data Link Working Group
- 33+ other Fora

Interoperability Programs

Information
Technology
Interoperability

DoN	Joint	Allied/NATO	Coalition
<ul style="list-style-type: none"> • Information Technology for the 21st Century (IT-21) • JMCIS98/GCCS-M • JTIDS/TADIL J • BGPHE/CHBDL • Radiant Mercury; C2G • DMS 	<ul style="list-style-type: none"> • Information Data Management (IDM) • Integrated Broadcast Service (IBS) • Global Command & Control System (GCCS) • Improved Data Link Standards <ul style="list-style-type: none"> • TADIL J • CHBDL • Radiant Mercury; C2G • DMS 	<ul style="list-style-type: none"> • Information Exchange Memoranda (IEM) • TACCIMS (Korea) • CSS (U.K.) • CRONOS (NATO) • MIDS • Radiant Mercury; C2G • X.400 e-mail 	<ul style="list-style-type: none"> • Radiant Mercury; C2G 

Interoperability Programs

The Panel identified numerous programs that show significant potential to enhance interoperability. The common thread throughout these programs is the drive to use widely accepted standards and a COTS approach wherever possible. The ubiquity of inexpensive, powerful commercial IT will allow the "perceived" gap in technology and interoperability between the US and our NATO, Allied and coalition partners to close and will ultimately be a key factor in achieving a level playing field for all.

Current qualitative assessment of interoperability would depict the level and capability as progressively decreasing as you move from:

- the individual services (Navy, Marine Corps, Army, and Air Force) to
- the Joint Services to
- NATO, Allied partners to
- coalition partners.

Program descriptions are provided in Appendix C.

The Panel identified numerous programs that show significant potential to enhance interoperability. The common thread throughout these programs is the drive to use widely accepted standards and a COTS approach wherever possible. The urgency of inexpensive, powerful commercial IT will allow the "perceived" gap in technology and interoperability between the US and our NATO, Allied and coalition partners to close and will ultimately be a key factor in achieving a level playing field for all.

Current qualitative assessment of interoperability would depict the level and capability as progressively decreasing as you move from:

- the individual services (Navy, Marine Corps, Army, and Air Force) to
- the Joint Services to
- NATO, Allied partners to
- coalition partners.

Program descriptions are provided in Appendix C.

Interoperability Programs			
Coalition	Allied/NATO	Joint	DoD
<ul style="list-style-type: none"> Information Exchange Information (IIR) TACCEM (IIR) CSS (IIR) CSS (IIR) 	<ul style="list-style-type: none"> Information Exchange Information (IIR) TACCEM (IIR) CSS (IIR) CSS (IIR) 	<ul style="list-style-type: none"> Information Exchange Information (IIR) TACCEM (IIR) CSS (IIR) CSS (IIR) 	<ul style="list-style-type: none"> Information Exchange Information (IIR) TACCEM (IIR) CSS (IIR) CSS (IIR)
<ul style="list-style-type: none"> Information Exchange Information (IIR) TACCEM (IIR) CSS (IIR) CSS (IIR) 	<ul style="list-style-type: none"> Information Exchange Information (IIR) TACCEM (IIR) CSS (IIR) CSS (IIR) 	<ul style="list-style-type: none"> Information Exchange Information (IIR) TACCEM (IIR) CSS (IIR) CSS (IIR) 	<ul style="list-style-type: none"> Information Exchange Information (IIR) TACCEM (IIR) CSS (IIR) CSS (IIR)



Procedures for Improving Interoperability

Information
Technology
Interoperability

- Doctrine/experiments
- Demonstrations
- Exercises
- Education and training
- Certification process
- Technology transfer
- Security/releasability

Current procedures should be enhanced

Procedures for Improving Interoperability

The Panel noted that there are several procedures and processes in place, which serve to improve interoperability. All of these need continued emphasis and direction. Procedures include:

Doctrine/Experiments

Interoperability must be an integral part of doctrine as it is developed and promulgated. This will serve to ensure that interoperability is thoroughly embedded in the very foundation of how the Navy trains and fights. The Fleet Battle Experiments (FBEs) provide an opportunity to verify how successful the DON has been in ensuring implementation of this important requirement. The FBE history/plan is as follows:

FBE "Alfa"	C3F	Mar 97	Completed
FBE "Bravo"	C3F	Sept 97	Completed
FBE "Charlie"	C2F	Apr 98	Completed
FBE "Delta"	C7F	Oct 98	
FBE "Echo"	C3F	Mar 99	

Demonstrations/Education and Training

Navy and Marine Corps cooperative efforts with the sea, land, and air forces of NATO, Allied and coalition partners are essential to the successful interoperability between nations. The enhanced relationships and interoperability gained through major multinational and bilateral exercises (160 major exercises with 64 different countries in 1996) increase US capability and credibility in forming and maintaining coalition partnerships to deter aggression and control crises.

Key demonstrations and exercises are designed to enhance interoperability and proficiency of multinational and bilateral forces. Examples include the following:

- Joint Warfare Interoperability Demonstration (JWID)
- ACTD's (i.e. C⁴I for Coalition Warfare)
- Strong Resolve - Second Fleet (SECONDFLT)
- Cooperation Afloat Readiness and Training (CARAT)
- Rim of the Pacific Exercise (RIMPAC) (THIRDFLT)
- Joint Task Force Exercises (JTFEX's)
- Partners for Peace Exercises (PiPEX's)
- Hunter/Urban Warrior

Finally, countries that intend to participate in coalition warfare operations must prepare in advance. This requires training exercises that must be carried out now. It is, after all, too late to try to improve operational cooperation and eliminate certain shortcomings at the start or even during an ongoing operation. Training with each other now in peacetime will foster the necessary level of professionalism and effectiveness needed to carry out an actual operation successfully.

Education & Training

Education and training processes which will enhance interoperability include formal schools and foreign exchange tours. Including NATO, allied and coalition participation in our formal schooling process increases awareness of interoperability issues.

Foreign exchange tours may provide increased understanding of interoperability issues.

Certification Process

Certification provides the warfighter with C⁴I systems that are interoperable and enables forces to exchange information effectively during a joint mission. Specifically, certification by the Test Command is confirmation that: (1) C⁴I system has undergone appropriate testing; (2) the applicable requirements for interoperability have been met; and (3) the system is ready for joint use. However, while a system may pass certification testing, it may not have been tested against all systems with

which it may eventually interoperate. This is because some systems with which they must interoperate become available later and commanders sometimes use systems in new ways that were not envisioned during testing.

Three organizations that focus on interoperability certification are: the JITC, the NCTSI and MCTSSA.

Additionally, the Panel generally concurs with the March 1998 Government Accounting Office (GAO) report titled "Joint Military Operations - Weaknesses in DoD's Process for Certifying C⁴I Systems' Interoperability." Two of the key items from this report were the need to enforce the interoperability and certification requirements and the need to improve the process for certifying C⁴I interoperability.

Technology Transfer

The technology transfer process must be streamlined. Common hardware and software can ensure interoperability. The ability of NATO, Allies and coalition partners to acquire US equipment in a straight forward, timely manner is crucial.

A technology "roadmap" can provide the direction the US must head and provide the associated interface specifications.

Security/Releasability

Security and releasability issues were identified as major roadblocks to interoperability. Adopting the SABI process is needed to develop more effective procedures and work around to alleviate this problem.

which it may eventually interoperate. This is because some systems with which they must interoperate become available later and commanders sometimes use systems in new ways that were not envisioned during testing.

Three organizations that focus on interoperability certification are the JIC, the NETS and MCTSA.

Additionally, the Panel generally concurs with the March 1998 Government Accounting Office (GAO) report titled "Joint Military Operations - Weaknesses in DoD's Process for Certifying C² Systems' Interoperability." Two of the key items from this report were the need to enhance the interoperability and certification requirements and the need to improve the process for certifying C² interoperability.

Technology Transfer

The technology transfer process must be streamlined. Common hardware and software can ensure interoperability. The ability of NATO, allies and coalition partners to acquire US equipment is a strategic forward. timely transfer is critical.

A technology "roadmap" can provide the direction the US must head and provide the associated interface specifications.

Security/Reliability

Security and reliability issues were identified as major roadblocks to interoperability. Adopting the SABR process is needed to develop more effective procedures and work around to alleviate this problem.

Plans & Procedures Recommendations

*Information
Technology
Interoperability*

- **ASD(C4ISR) designate a single US authority for interoperability with NATO, Allied, and coalition forces**
- **DoN CIO appoint a Deputy to focus on NATO, Allied and coalition interoperability**
 - **CINCs promote international exercises/training and OPNAV/MCCDC ensure feedback to the acquisition system**
- **OPNAV N3/N6/N7 and CG MCCDC evaluate/validate interoperability improvements via an aggressive exercise/demonstration/training program**
- **ASD(C4ISR) should adopt SABI process for effective security/releasability procedures**
- **ASD(C4ISR)/DISA enforce interoperability and certification requirements as described in the March 1998 GAO report**

Plans and Procedures Recommendations

The Panel provides the following recommendations to mitigate the issues noted on the previous charts for plans and procedures:

- **ASD(C⁴ISR) in concert with CJCS and the CINCs, designate a single US authority for interoperability with NATO, Allied, and coalition forces. The reduction in US forces, combined with the increasing number of requirements (primarily - Operations Other Than War (OOTW)) make it imperative that US forces can interoperate with NATO, Allied and coalition forces. A single authority is required in order to more effectively coordinate joint interoperability efforts between the services and non-US forces.**
- **DON CIO appoint a Deputy to focus on NATO, Allied and coalition interoperability. Appointment of a Deputy will place increased emphasis on NATO, allied and coalition interoperability while simultaneously providing a single point of contact within the DON.**
- **CINCs promote international exercise/training and Chief of Naval Reserves (OPNAV)/MCCDC ensure feedback to the acquisition system.**

- OPNAV N3/N6/N7 and MCCDC evaluate/validate interoperability improvements via an aggressive exercise/demonstration/training program. Participation in exercises, demonstrations and training are crucial for ensuring that NATO, allied and coalition systems are, in fact, interoperable.
- ASD(C⁴ISR), in concert with the CJCS and the CINCs, should adopt SABI process for effective security/releasability procedures. Security/releasability was identified as a major interoperability problem; adoption of the SABI process can significantly reduce the administration and time requirements—thus speeding the fielding of interoperable systems.
- ASD(C⁴ISR)/DISA enforce interoperability and certification requirements as described in the March 1998 GAO report. The DoD does not have an effective process for certifying existing, newly developed, and modified C⁴I systems for interoperability. Improvements to the certification process are needed to provide better assurance that C⁴I systems are tested and certified for interoperability.

Plans and Procedures Recommendations

The Panel provides the following recommendations to mitigate the issues noted on the previous charts for plans and procedures:

- ASD(C⁴ISR) in concert with CJCS and the CINCs, designate a single US authority for interoperability with NATO, Allied, and coalition forces. The reduction in US forces, combined with the increasing number of requirements (primarily - Operations Other Than War (OOTW)) make it imperative that US forces can interoperate with NATO, Allied and coalition forces. A single authority is required in order to more effectively coordinate joint interoperability efforts between the services and non-US forces.
- DON CIO appoint a Deputy to focus on NATO, Allied and coalition interoperability. Appointment of a Deputy will place increased emphasis on NATO, allied and coalition interoperability while simultaneously providing a single point of contact within the DON.
- CINCs promote international exercise/training and C4I of Naval Forces (OPNAV)/MCCDC ensure feedback to the acquisition system.

Infosystem Interoperability "7-layer" Open Systems Model

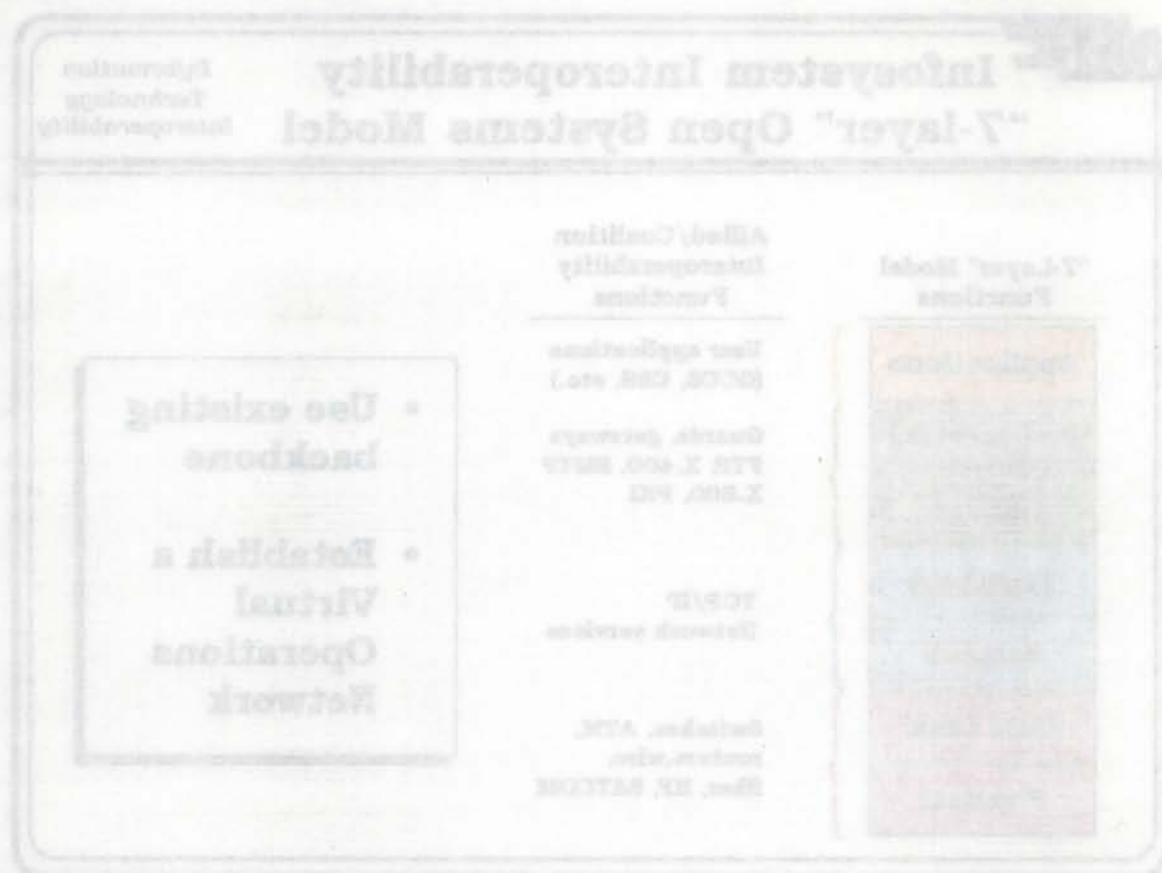
*Information
Technology
Interoperability*

"7-Layer" Model Functions	Allied/Coalition Interoperability Functions
Applications	User applications (GCCS, CSS, etc.)
Presentation	Guards, gateways FTP, X.400, SMTP X.500, PKI
Session	
Transport	TCP/IP
Network	Network services
Data Link	Switches, ATM, routers, wire, fiber, HF, SATCOM
Physical	

- **Use existing backbone**
- **Establish a Virtual Operations Network**

Infosystem Interoperability "7-Layer" Open Systems Model

The interface elements of the 7-layer open systems communication model and their correspondence to the interoperability functions are illustrated above. Within the context of this relationship (i.e. utilizing existing backbone and support infrastructure), it is proposed to establish a VON. This concept is specifically targeted at bringing existing technologies and commercial standards together to achieve a much higher level of interoperability than is presently available. As previously noted, the VON builds upon many of the concepts and objectives defined in the DON's IT-21 plans, as well as in the NATO CRONOS initiative.

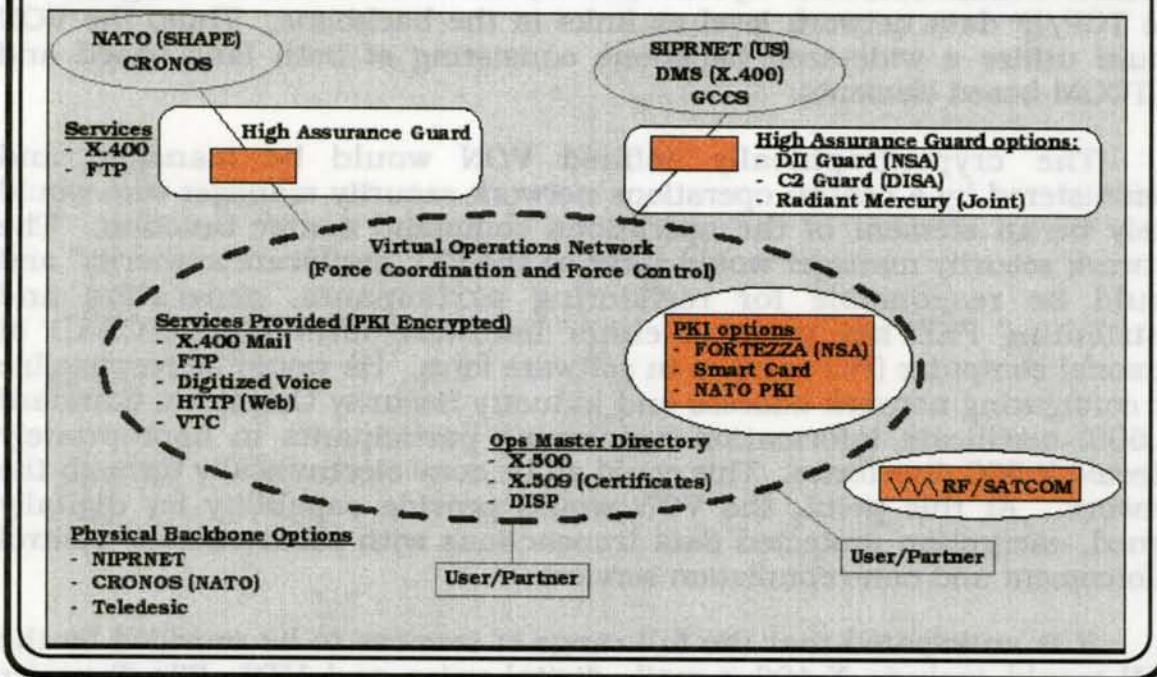


Information Interoperability "7-Layer" Open Systems Model

The interface elements of the 7-layer open systems communication model and their correspondence to the interoperability functions are illustrated above. Within the context of this relationship (i.e. utilizing existing backbone and support infrastructure), it is proposed to establish a VON. This concept is specifically targeted at bringing existing technologies and commercial standards together to achieve a much higher level of interoperability than is presently available. As previously noted, the VON builds upon many of the concepts and objectives defined in the DOW's IT-21 plan, as well as in the NATO CHRONOS initiative.

"Virtual Operations Network" Concept

Information
Technology
Interoperability



"Virtual Operations Network" (VON) Concept

It is recognized in this Study that to achieve and optimize information interoperability, it is necessary to integrate critical "enabling" technologies into an "interoperability support infrastructure" which can be defined, implemented, refined and eventually fielded. Such a support infrastructure has been conceptualized and refined within the limits of this study and is referred to as the VON concept. This VON concept builds upon many of the concepts and objectives defined in the DONs IT-21 initiative as well as in the NATO "CRONOS" initiative, and is intended to be compatible with those concepts. The VON concept is specifically targeted at bringing existing "enabling" technology and commercial standards together to achieve a much higher level of interoperability than is presently achieved with those concepts.

A top-level pictorial description of the VON concept is presented above. In this concept a "virtual" private network domain is established at the "application" level through the use of Public Key Encryption (PKE) technology. We would specifically suggest using the US-NSA supported (exportable) FORTEZZA PKE technology for this purpose although other equivalent NATO technology could also be used. Recent bandwidth improvements in the latest FORTEZZA implementations also make it a near-term usable candidate. In the context of an allied/coalition operation this

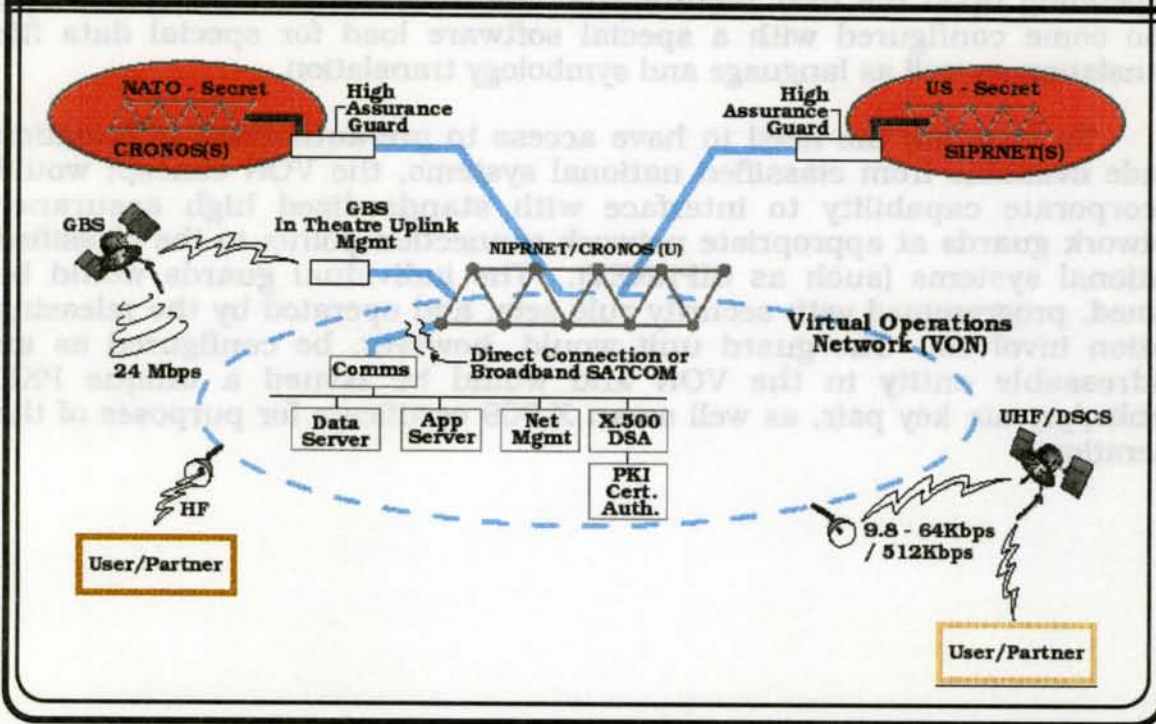
VON could be set up electronically using any mutually available TCP/IP-based physical network infrastructure. The unclassified US NIPRNET, or perhaps one of the NATO CRONOS networks, would be good candidates as a core wide-area backbone. To support anticipated mobile, "afloat" operations, specified channels of UHF SATCOM and perhaps Defense Satellite Communications System (DSCS) SATCOM would be integrated at the TCP/IP data network level as links in the backbone. Thus, the VON would utilize a wide-area backbone consisting of both land-based and SATCOM-based elements.

The cryptographically defined VON would be managed and administered by a central operations network security manager who would likely be an element of the operations command center function. The network security manager would serve as the PKI "certificate authority" and would be responsible for registering participants, generating and distributing PKE key pairs in either hardware form (SMARTCARD or personal computer (PC) card) or in software form. He would be responsible for configuring network address and Industry Security Certificate Standard (X.509) certificate information concerning participants in appropriately selected X.500 directories. This could all be done electronically through the network. At this point, the VON would provide capability for digitally signed, encryption protected data transactions with secure access control enforcement and non-repudiation services.

It is anticipated that the full range of services to be provided by the VON would include X.400 e-mail, digital voice and VTC, File Transfer Protocol (FTP)-based file transfer services and some level of Hyper Text Transport Protocol (HTTP)-based web services. Not all participants would require this full range of services. The specific services allowed to each user would be specified in their individual X.509 certificate and controlled by security services provided by the PKE enforcement mechanisms.

Command Center Functions within "VON"

Information
Technology
Interoperability



Command Center Functions Within "VON"

The VON administration and security management functions which would likely be associated with the command center operation are shown above. The command center might be physically located either "ashore" or "afloat." If shore-based, its VON interface would be direct connection into the land-based backbone (NIPRNET, etc.). If the command center were "afloat," it would likely be deployed on a command ship (such as the USS BLUE RIDGE) so that the connection to the backbone would utilize broadband SATCOM such as DSCS.

Using the NIPRNET or similar network as the basic backbone, it would be possible to easily integrate GBS services as part of the VON using standard network connectivity and services to the appropriate GBS uplink management center. All critical participants in the VON, including the GBS uplink center, would be issued the FORTEZZA-based encryption in either hardware or software form so that all transactions are digitally signed, audited and encryption protected.

In the VON concept it would be very desirable to develop and deploy a standardized "VON terminal set." The VON terminal set would consist of a low profile UHF SATCOM antenna receiver and a VON interface processor. The VON interface processor would consist of a high-end PC which provides

TCP/Joint Publication (JP) network interfacing, would support either hardware-based (PC card) or software-based PKE encryption services, digitized voice and VTC interfaces, Local Area Network (LAN) connectivity, as well as X.400 e-mail, and word processing, and PowerPoint style graphics. Depending upon the user requirement, the VON interface processor may also come configured with a special software load for special data file translation as well as language and symbology translation.

To facilitate the need to have access to pre-authorized information made available from classified national systems, the VON concept would incorporate capability to interface with standardized high assurance network guards at appropriate network connection points to the classified national systems (such as SIPRNET). The individual guards would be owned, programmed with security rule sets, and operated by the releasing nation involved. The guard unit would, however, be configured as an addressable entity in the VON and would be issued a unique PKE public/private key pair, as well as an X.509 certificate for purposes of the operation.



Command Center Functions Within "VON"

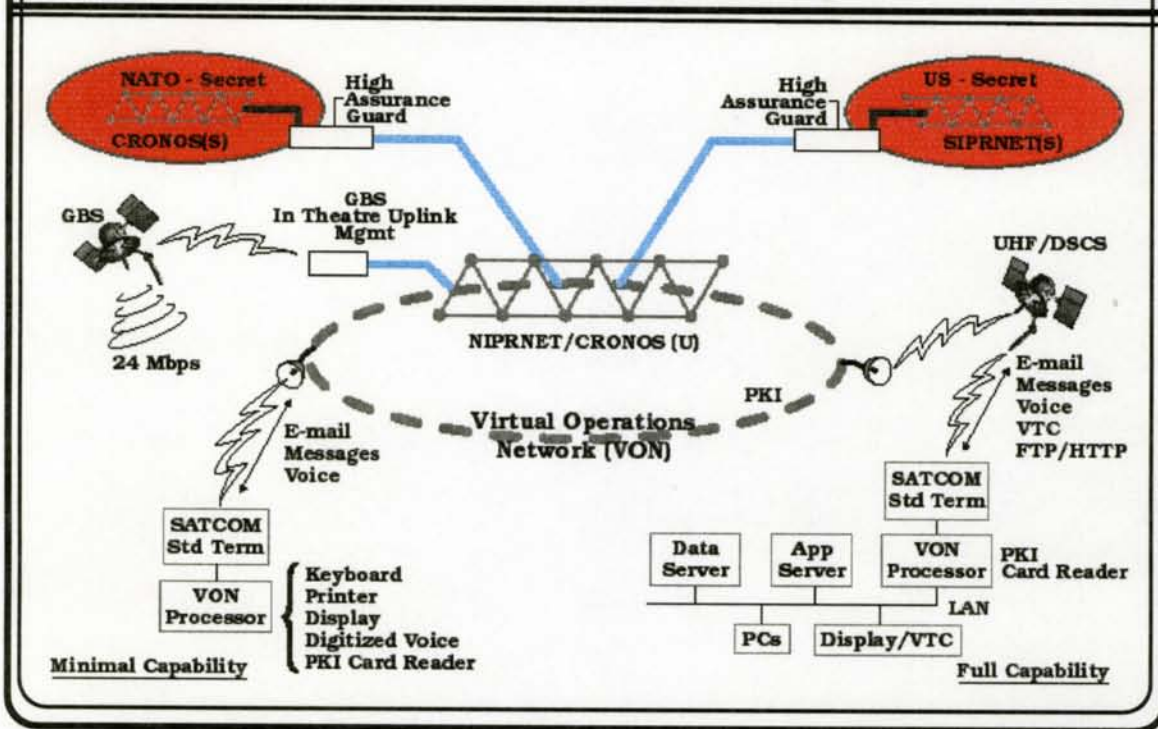
The VON administration and security management functions which would likely be associated with the command center operation are shown above. The command center might be physically located either "on-site" or "off-site." If "on-site," the VON interface would be direct connection into the land-based backbone (SIPRNET, etc.). If the command center were "off-site," it would likely be deployed on a command ship (such as the USS BLUE WING) so that the connection to the backbone would utilize broadband SATCOM such as DSCS.

Using the SIPRNET or similar network as the basic backbone, it would be possible to easily integrate GDS services as part of the VON using standard network connectivity and services to the appropriate GDS uplink management center. All critical participants in the VON, including the GDS uplink center, would be issued the FORTEZZA-based encryption in either hardware or software form so that all transactions are digitally signed, audited and encryption protected.

In the VON concept it would be very desirable to develop and deploy a standardized "VON terminal set." The VON terminal set would consist of a low profile UHF SATCOM antenna receiver and a VON interface processor. The VON interface processor would consist of a high-end PC which provides

User/Partner Function Capability

Information
Technology
Interoperability

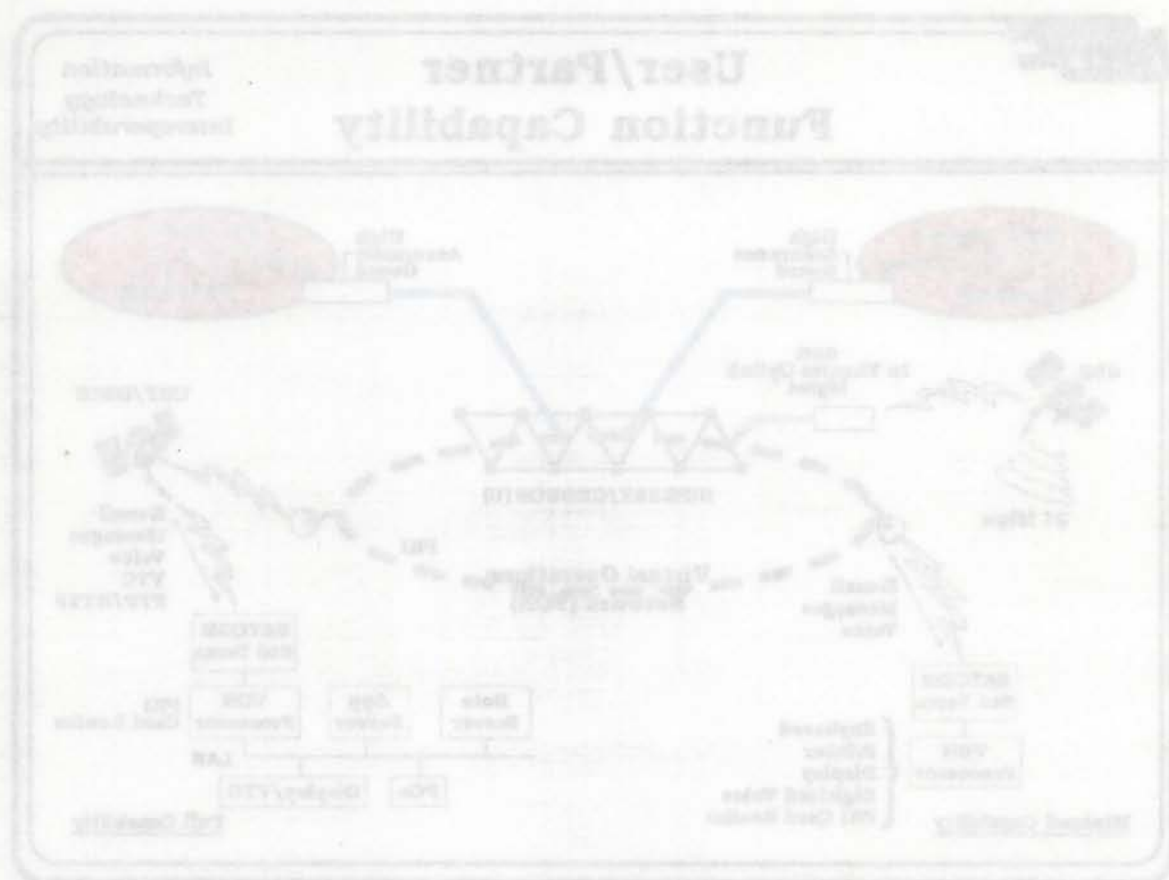


User/Partner Function Capability

As indicated earlier, it is not anticipated that all participants in an operation would require the full range of VON services depending upon individual mission role. The above chart illustrates the range of VON user terminal support functions from a minimal capability that supports e-mail, messaging, and digitized voice to a full capability similar to that provided to the command center.

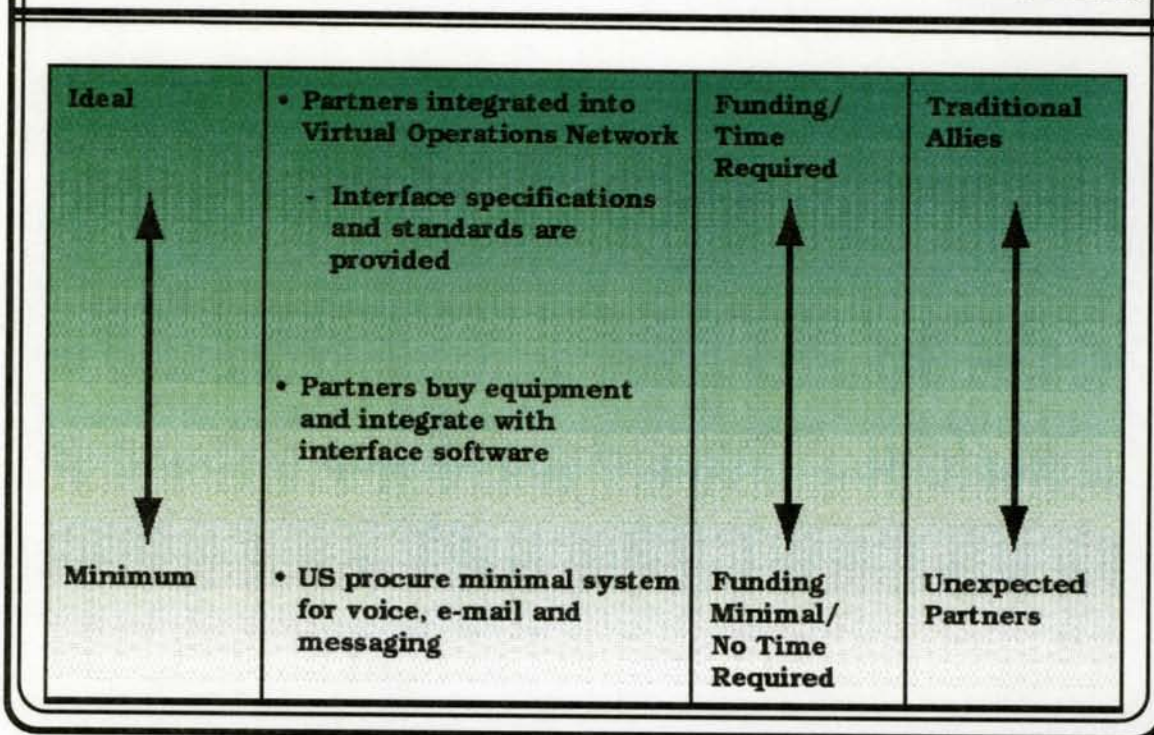
As indicated earlier, it is not anticipated that all participants in an operation would require the full range of VON services depending upon individual mission role. The above chart illustrates the range of VON user (remote) support functions from a minimal capability that supports e-mail, messaging, and digitized voice to a full capability similar to that provided to the command center.

User/Partner Function Capability



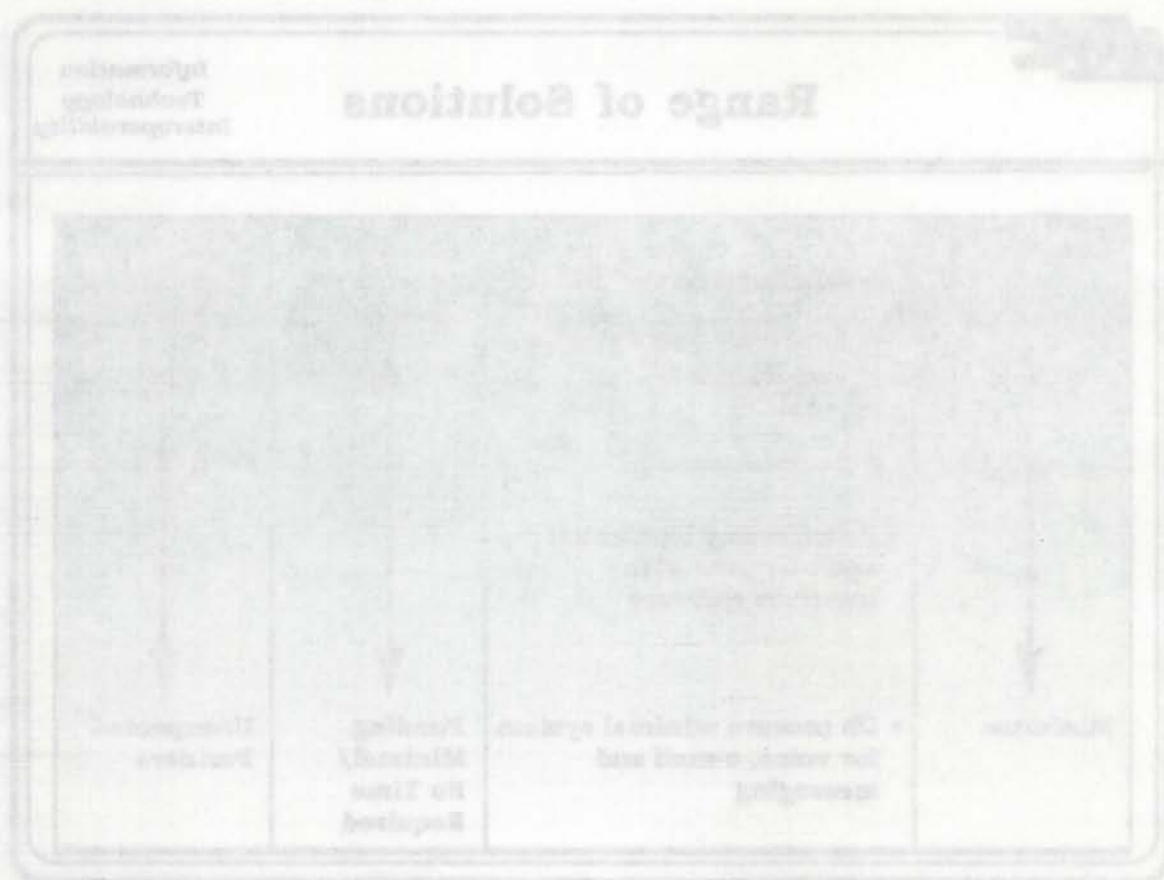
Range of Solutions

Information
Technology
Interoperability



Range of Solutions

It is expected that the traditional major Allies would have full VON participation capability including secure e-mail, voice, VTC and FTP/HTTP Web services. Other coalition partners in a specific operation may not require full VON services capability, depending upon their role in the mission. In some such cases capabilities for secure e-mail and voice communications would be sufficient. The above chart illustrates the expectation that the larger traditional Allies would very likely procure their own VON interfacing system from their own national industrial base using standardized interface specifications established by the major Allies (i.e. NATO, etc.). Smaller partner nations could also procure VON interface systems from producer nations and integrate them for their own operational use. The US and some of the traditional Allies should additionally procure and stockpile a number of "low-end" VON terminal equipment capable of supporting secure voice and e-mail services. In a time of crisis this equipment could be quickly distributed to coalition partners as required to help achieve adequate levels of force interoperability with minimal lead-time.



Range of Solutions

It is expected that the traditional major Allies would have full VON participation capability including secure e-mail, voice, VTC and FTS/PTT/ Web services. Other coalition partners in a specific operation may not require full VON services capability, depending upon their role in the mission. In some cases capabilities for secure e-mail and voice communications would be sufficient. The above chart illustrates the expectation that the larger traditional Allies would very likely procure their own VON interlinking system from their own national industrial base using standardized interface specifications established by the major Allies (i.e., NATO, etc.). Smaller partner nations could also procure VON interlinking systems from producer nations and integrate them for their own operational use. The US and some of the traditional Allies should additionally procure and stockpile a number of "low-end" VON external equipment capable of supporting secure voice and e-mail services. In a time of crisis this equipment could be quickly distributed to coalition partners as required to help achieve adequate levels of force interoperability with minimal lead-time.

"Enabling" Technologies

*Information
Technology
Interoperability*

- **Commercial network protocols**
- **Releasable public key encryption technology**
- **High assurance network "releasability guard" technology**
- **Network intrusion detection and defense technology**

"Enabling" Technologies

There are several enabling technologies which will reduce the technology obstacles to NATO, Allied and coalition forces interoperability. Utilization of commercial network protocols, COTS standards and services combine into a critical common denominator for information systems interoperability. These include TCP/IP, System Network Management Protocol (SNMP), HTTP, X.500, etc. PKE technology is also needed to provide for the secure exchange of information among a subset of network users, on a need-to-know basis. PKE technology must be electronically distributed and managed and be compatible with COTS TCP/IP network operations. High assurance network guard technology is required to provide for rigid security control in automating the downgrading and release process of authorized data files from classified national systems, such as SIPRNET, to Allied, and coalition partners on a need-to-know basis; examples include Radiant Mercury guard, the Standard Command and Control guard (C2G(US-DISA)/VS - DISA) and the standard high assurance E-mail guard for both X.400 and SMTP protocols which is available from NSA. Advanced software technologies for detection of network intrusion must also be incorporated in a secure interoperability capability.

"Enabling" Technologies

- Commercial network protocols
- Releaseable public key encryption technology
- High assurance network "releaseability" guard technology
- Network intrusion detection and defense technology

"Enabling" Technologies

There are several enabling technologies which will reduce the technology obstacles to NATO, Allied and coalition forces interoperability. Utilization of commercial network protocols, COTS standards and services combine into a critical common denominator for information systems interoperability. These include TCP/IP, System Network Management Protocol (SNMP), HTTP, X.400, etc. PKE technology is also needed to provide for the secure exchange of information among a subset of network users, on a need-to-know basis. PKE technology must be electronically distributed and managed and be compatible with COTS TCP/IP network operations. High assurance network guard technology is required to provide for rigid security control in automating the downgrading and release process of authorized data files from classified national systems, such as SIPRNET, to Allied, and coalition partners on a need-to-know basis. Examples include Radiant Mercury Guard, the Standard Command and Control Guard (SCCUS-DISA) V2 - D2A, and the standard high assurance E-mail guard for both X.400 and SMTP protocols which is available from NSA. Advanced software technologies for detection of network intrusion must also be incorporated in a secure interoperability capability.

- **Interface and management technology for GBS utilization**
- **Programmable high performance data format translation technology / language translation**
- **Commercial SATCOM technology as backup for minimal voice comms**
- **TCP/IP network compatibility for enhanced UHF SATCOM**

"Enabling" Technologies

Effective use of GBS requires improved development of technologies for context allocation and bandwidth management. Software-based data translation tools (eventually, language translation tools), so-called interoperable by middleware, are needed to interact at a process-to-process level through networks. These tools provide automated translation of data structures and formats and require standardized configuration control. In addition, specific technologies should be developed to make commercial SATCOM a military backup for voice communication as well as to make UHF SATCOM communication compatible with data networks in the sense of TCP/IP network compatibility.

"Enabling" Technologies

- Interface and management technology for
GIS utilization
- Programmable high performance data format
translation technology / language translation
- Commercial SATCOM technology as backup
for minimal voice comms
- TCP/IP network compatibility for enhanced
UDP SATCOM

"Enabling" Technologies

Effective use of GIS requires improved development of technologies for content allocation and bandwidth management. Software-based data translation tools (eventually, language translation tools), so-called interoperable by middleware, are needed to interact at a process-to-process level through networks. These tools provide automated translation of data structures and formats and require standardized configuration control. In addition, specific technologies should be developed to make commercial SATCOM a primary backup for voice communication as well as to make UDP SATCOM communication compatible with data networks in the sense of TCP/IP network compatibility.

- **SPAWAR establish, demonstrate and refine a Virtual Operations Network (VON) capability with**
 - TCP/IP Network compatibility
 - Video teleconferencing
 - Bandwidth on demand
 - GBS interface
 - Automated message and language translators
 - PKI security services
- **ASD(C4ISR) utilize Public Key Encryption Infrastructure (PKI) technology**
- **DASN(C4I) adopt and enhance high assurance, programmable guard technology**
 - Accelerate approval process as a SIPRNET interface
 - Promote early release of secure systems (via NSA/SABI, international fora)

Technical Recommendations

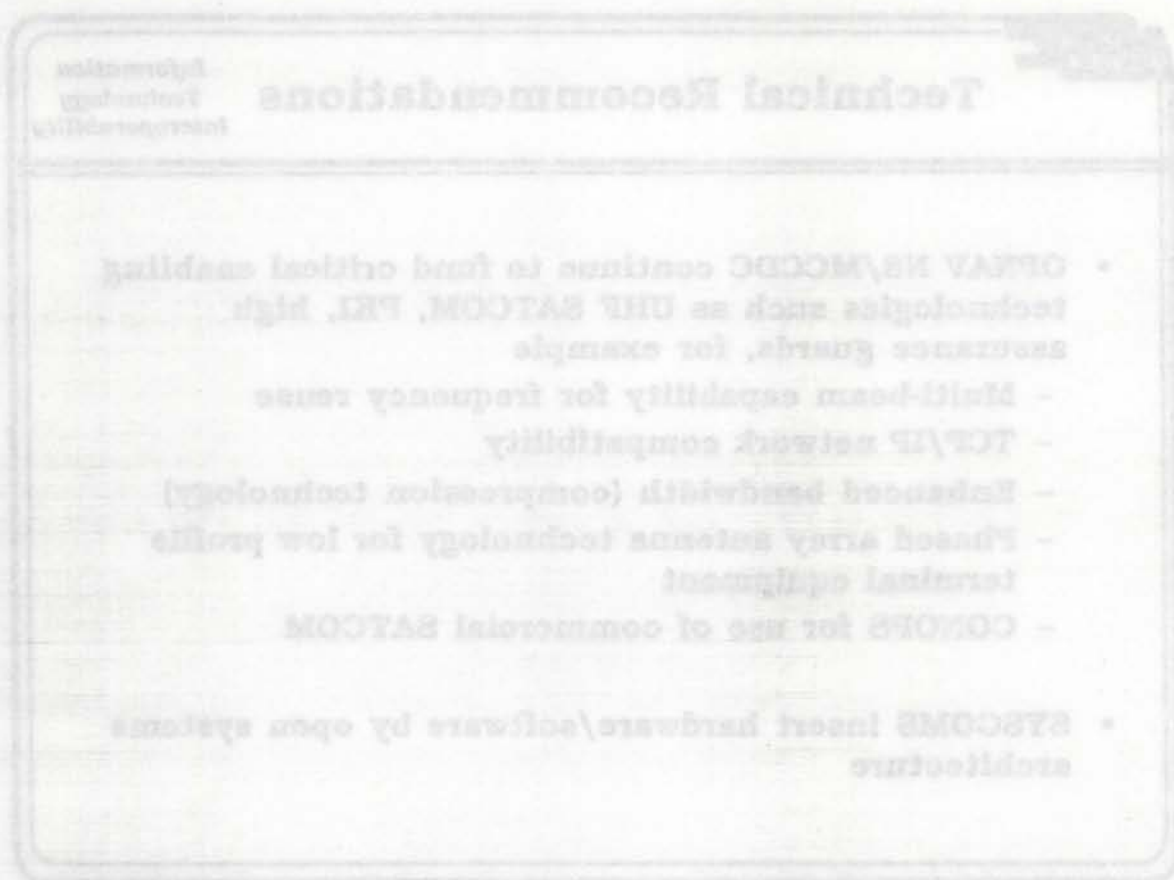
The study's key technical recommendations to achieve the proposed varying degree of interoperability, minimum to ideal, are listed above. Critical to this goal is the utilization of existing COTS capabilities and the further aggressive development of accredited secure support infrastructure, primarily the PKI and high assurance guard technologies. In addition, a more effective approval process than presently available is required for timely release of high assurance guards as a SIPRNET interface as well as early release of security technology via the NSA's SABI. The VON concept became the keystone of this study to providing a secure tactical infrastructure for communications services which is critical for interoperability.

- **OPNAV N8/MCCDC continue to fund critical enabling technologies such as UHF SATCOM, PKI, high assurance guards, for example**
 - **Multi-beam capability for frequency reuse**
 - **TCP/IP network compatibility**
 - **Enhanced bandwidth (compression technology)**
 - **Phased array antenna technology for low profile terminal equipment**
 - **CONOPS for use of commercial SATCOM**
- **SYSCOMS insert hardware/software by open systems architecture**

Technical Recommendations

The key technology recommendations made in this study focus on maturing and integrating "enabling" technologies necessary to provide a critical set of secure, interoperable services to support allied and coalition operations. Perhaps the most critical of these recommendations is that to exploit and apply PKE technology and high assurance network guard technology, which is central to being able to secure interoperable transactions and to facilitate controlled releasability of information across national security boundaries.

Using PKE technology and COTS network technology, this study strongly recommends that a VON capability be established and refined. Because of the criticality of SATCOM communications as an integral part of such a VON capability, it is further recommended that enhancements be made in near-term UHF SATCOM, including multi-team capability for frequency reuse, enhanced bandwidth, low profile phased array antenna technology. It is also important that CONOPS be developed for effective utilization of commercial SATCOM and GBS systems and that open systems architecture be adopted for all future hardware/software acquisitions.



Technical Recommendations

The key technology recommendations made in this study focus on meeting and integrating "enabling" technologies necessary to provide a critical set of secure, interoperable services to support allied and coalition operations. Perhaps the most critical of these recommendations is that to exploit and apply PKE technology and high assurance network guard technology, which is central to being able to secure interoperable transactions and to facilitate controlled releasability of information across national security boundaries.

Using PKE technology and COTS network technology, this study strongly recommends that a VON capability be established and refined. Because of the criticality of SATCOM communications as an integral part of such a VON capability, it is further recommended that enhancements be made in near-term UHF SATCOM, including multi-beam capability for frequency reuse, enhanced bandwidth, low profile phased array antenna technology. It is also important that CONOPS be developed for effective utilization of commercial SATCOM and GPS systems and that open systems architecture be adopted for all future hardware/software acquisitions.

- **US Forces must operate with NATO, Allied and coalition forces**
- **Continue to promote network technology**
- **Protect classified information**
- **Demand interoperability in acquisition/training process**

Strategy

As a result of the study, this Panel recommends the above strategy for the DON:

- US Forces must continue to operate with NATO, allied and coalition forces in order to augment the force effectiveness of US forces in the Joint Vision 2010
- Continue to promote network technology in order to gain the benefits of rapid technology insertion while shifting the paradigm to Network Centric Warfare
- Protect classified information. Any interoperability improvements must not come at the expense of security of each nation's sensitive information
- Demand interoperability both in the acquisition process and in training

Strategy

- US Forces must operate with NATO, Allied and coalition forces
- Continue to promote network technology
- Protect classified information
- Demand interoperability in acquisition/training process

Strategy

As a result of the study, this Panel recommends the above strategy for the DoD:

- US Forces must continue to operate with NATO, allied and coalition forces in order to augment the force effectiveness of US forces in the Joint Vision 2010
- Continue to promote network technology in order to gain the benefits of rapid technology insertion while shifting the paradigm to Network Centric Warfare
- Protect classified information. Any interoperability improvements must not come at the expense of security of each nation's sensitive information
- Demand interoperability both in the acquisition process and in training

Strategy

- **US Forces must operate with NATO, Allied and coalition forces**

Recommendations

- **ASD(C4ISR) designate a single US authority to be proactive on interoperability issues with NATO, Allied and coalition forces**
- **DASN(C4I)/OPNAV N6/MCCDC should actively participate in all NATO interoperability fora**
 - **DoN CIO appoint a Deputy to focus on NATO, allied and coalition interoperability**

Strategy and Recommendations

The above chart provides the strategy and associated recommendations provided by the Panel.

As the US Navy and Marine Corps continue to downsize their forces while still facing global challenges, force effectiveness will be enhanced through information dominance, as articulated in Joint Vision 2010. Additional force effectiveness can be achieved through employment of other maritime forces in NATO, allied and coalition Joint Task Forces. Therefore, there is a strategic national and naval imperative to enhance interoperability with these forces.

Interoperability concerns are being addressed in various fora. Current strong emphasis is being placed on system, platform and Joint interoperability. However, throughout the Panel briefings it became apparent that there is no single authority for establishing policy and enforcing NATO, allied and coalition interoperability for US Navy or other services' information technology systems.

The Panel recommends that a single authority for NATO, allied and coalition interoperability be empowered. CINCUSACOM/SACLANT is the suggested focal point for this authority. With dual NATO and JCS

responsibility, Atlantic Command (ACOM) would have the broadest scope of authority with regard to implementation and enforcement of interoperability standards.

Recent coalition operations in the Gulf and Bosnia have demonstrated that NATO standards promote interoperability among coalition nations where standards are lacking. Naval Forces need to be more proactive in NATO Interoperability Standards Working Groups which are developing standards that often are not interoperable with US standards. The current level of US Naval involvement in these working groups does not adequately support developing new IT systems which are interoperable with NATO.

Strategy

- **Continue to promote network technology**

Recommendations

- **SPAWAR establish, demonstrate and refine a Virtual Operations Network (VON) capability**
- **OPNAV N8/MCCDC continue to fund critical enabling technologies such as UHF SATCOM, PKI, high assurance guards**
- **SYSCOMs insert hardware/software by open systems architecture approach**

Strategy and Recommendations

The above chart provides the strategy and associated recommendations provided by the Panel.

The rapid growth in IT, and its enabling elements for processing and communication, underscores several needs for the Navy and Marine Corps. The DON must maintain technological currency and insert the technology on an "as available" basis to mitigate systems obsolescence and interoperability shortfalls. Examples are programmable high performance data format translation and automated natural language translation technologies. At the same time, the technology must be integrated with a focus on interoperability in order to gain and maintain full operational leverage. Unfortunately, this same rapid technological growth can introduce major operating difficulties when interoperability is not considered on the same par as performance at the outset. As a result, the operational Fleet may consider the technology at fault, as opposed to the process.

The Panel believes that the DON must continue to aggressively pursue advances in IT, while providing a focus on interoperability of the technology elements for operational leverage. Proper balance in these two areas will ensure cost savings and operational effectiveness.

The Panel recommends that the DON take several steps to enhance the process, capture the technology benefits, and emphasize interoperability:

- DASN(C⁴I)/CIO can provide focused leadership for interoperability of IT by appointment of a Deputy CIO responsible for interoperability with NATO, allied and coalition forces. This position must have direct access to ASN(RD&A) and DASN (C⁴I)/CIO. The Deputy CIO should have responsibility, authority and accountability to oversee the interoperability of IT and rapid, timely insertion of IT advances which emphasize interoperability of resulting systems and subsystems in the design, development, and throughout the acquisition process.
- DASN(C⁴I)/CIO should expand efforts to include the results of Information and Network Technology initiatives from other government agencies and from industry. The Panel generally concurs with the recommendations of the GAO Draft Report, "Joint Military Operations: Navy Command and Control Systems Not Certified as Interoperable," dated 23 January 1998.
- DON should continue to fund Research and Development (R&D) for "defense unique" IT needs and applications, while also providing funding for the maximum practical use and integration of commercially developed technology. Concepts of operations should be developed for the use of commercial SATCOM as a backup for minimal voice communications. Such investments must be tied with an acquisition strategy that enables the Fleet to maintain technology currency. The use of an open architecture approach for the technology, and resulting hardware and software, will facilitate integration on a more frequent and orderly basis and should result in significant Operations and Maintenance (O&M) cost savings. As part of this process, the Panel recommends the DON implement a technology insertion plan for fleet information systems. This should be based upon interoperability needs and requirements from an approved interoperability plan, selected critical systems and subsystems consonant with DoD's Joint Technical Architecture (JTA), and an open systems approach. For example, technology for the interface, management and utilization of the GBS requires such a technology insertion plan.
- DON should invest in the implementation of the JTA, open systems approaches, and insertion of COTS (hardware and software) technology, including common modular and reusable software. The DON implementation strategy must seek "targets of opportunity" for insertion of the technology into legacy systems while emphasizing interoperability among all fleet assets as both a technology strategy and as an acquisition strategy. "Hooks" must be provided for interoperability considerations when introducing new equipment, and hardware and software upgrades.
- DON should invest in critical "stopgap" or "workaround" systems, subsystems, and equipment for distribution to Allied and coalition forces

as necessary to ensure that minimum critical levels of interoperability are met on a timely basis for rapid deployment and buildup of military forces.

- SPAWAR should define a VON to provide reliable connectivity while being responsive to an individual nation's security concerns and provide a systems demonstration in NATO, allied and coalition operations. This VON would be developed in a TCP/IP Multi-Network Environment using FORTEZZA-based PKE infrastructure. This network would provide for the secure transfer of data/voice from national classified networks, such as SIPRNET, Linked Operational Intelligence Centers Europe (LOCE), etc., using high assurance network guards. The VON would form a virtual private network for operations control, providing e-mail (X.400), HTTP web based services, digitized VTC services and Common Operational Picture. The architecture should be implemented using COTS systems, such as servers and PCs, with software employing commercial open standards. This VON will promote interoperability by lowering the barriers for designated coalition partners to acquire their own national systems which are compliant with internationally recognized standards in a fiscally constrained environment. The VON interoperability concept will also reduce the time required for training of the systems if they are reflective of other commercial systems in their nations. In a crisis, the DON should be prepared to provide minimum essential equipment to coalition partners to achieve minimum essential C² interoperability.
- DON should aggressively use interoperability demonstrations and fleet exercises with Allied and coalition forces as "targets of opportunity" for evaluation of interoperability and extend such demonstrations and exercises to include relevant ACTDs whenever practical. Also, the Panel recommends that Development, Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) be expanded to include integrated allied and coalition operations which focus on and test interoperability. The objectives of such operations and evaluations are to properly demonstrate and refine interoperability needs, requirements, and benefits for Information and network technologies.
- DON should develop SATCOM technology to provide near-term enhanced UHF multi-beam and digital voice capability, and to incorporate data compression techniques. All prospective VONs and SATCOM should be TCP/IP network compatible.

as necessary to ensure that minimum critical levels of interoperability are met on a timely basis for rapid deployment and buildup of military forces.

STANAG should define a VON to provide reliable connectivity while being responsive to an individual nation's security concerns and provide a systems demonstration in NATO, allied and coalition operations. This VON would be developed in a TCP/IP Multi-Network Environment using FORTEZA-based PKE infrastructure. This network would provide for the secure transfer of data/voice from national classified networks, such as SIPRNET, Linked Operations Intelligence Centers Europe (LOICE), etc., using high assurance network guards. The VON would form a virtual private network for operations control, providing e-mail (X.400), HTTP web based services, digitized VTC services and Common Operational Picture. The architecture should be implemented using COTS systems, such as servers and PCs, with software supporting connected open standards. This VON will promote interoperability by lowering the barriers for designated coalition partners to acquire their own national systems which are compliant with internationally recognized standards in a locally-contained environment. The VON interoperability concept will also reduce the time required for training of the systems if they are reflective of other commercial systems in their nations. In a crisis, the VON should be prepared to provide minimum essential equipment to coalition partners to achieve minimum essential interoperability.

DON should aggressively use interoperability demonstrations and exercises with allied and coalition forces as "targets of opportunity" for evaluation of interoperability and extend such demonstrations and exercises to include relevant ACTDs whenever practical. Also, the Panel recommends that Development, Test and Evaluation (DT&E) and Operational Test and Evaluation (OT&E) be expanded to include integrated allied and coalition operations which focus on and test interoperability. The objectives of such operations and evaluations are to properly demonstrate and refine interoperability needs, requirements, and benefits for information and network technologies.

DON should develop SATCOM technology to provide near-term enhanced UHF multi-beam and digital voice capability, and to incorporate data compression techniques. All prospective VONs and SATCOM should be TCP/IP network compatible.

Strategy

- **Protect classified information**

Recommendation

- **ASD(C4ISR) utilize Public Key Encryption Infrastructure (PKI) technology**
- **DASN(C4I)/OPNAV N6 adopt and enhance high assurance, programmable guard technology**
- **ASD(C4ISR) adopt SABI process for effective security/releasability procedures**

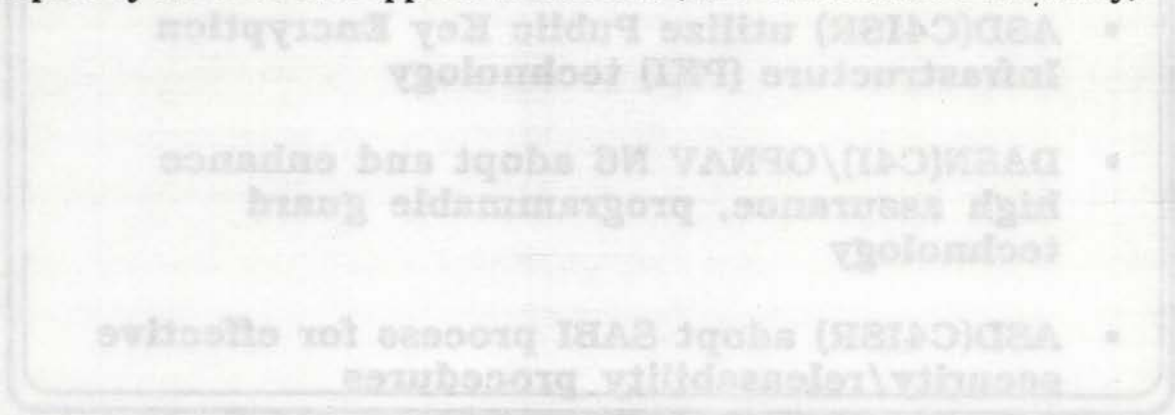
Strategy and Recommendations

The above chart provides the strategy and associated recommendations provided by the Panel.

A major assumption of the study, which was reinforced through all of the briefings, is the fundamental tenet that national information must be protected. As an example, this is the major obstacle to sharing the SIPRNET with NATO, Allied and coalition partners. The present systems have no agreed upon means of partitioning access. PKE technology with high assurance guard proxies allow secure, highly reliable systems which protect individual data for national participants within the context of managed risk. Recognizing that DON and national policies are not yet ready to restructure US classified nets, including SIPRNET, for partitioned access on need-to-know basis for Allied and coalition nations, the VON concept would meet the mission informational needs of the operational participants while protecting security.

The technology to support the use of PKE is maturing. Adoption of developments in industry and DoD/NSA in this area should provide both the infrastructure and the necessary level of security for military systems. Continued investment should be made in high assurance guard systems, incorporating the technologies already demonstrated and used by DISA,

NSA, and other agencies in conjunction with commercial industry. These products should be consolidated and standardized wherever possible and be incorporated as part of DoD's Common Operating Environment. Early release of secure systems should be promoted through NSA and international fora. The guards for gateways to other nations will be deployed and used under the control of those nations. Nations possessing technology sophistication will undoubtedly develop their own high assurance guard products in conjunction with common sets of interoperable interface specifications. For other nations, guard products can be provided by NATO or other agencies and the programming and control of the guards would be the responsibility of the receiving nations with their security rules applied. Effective security and releasability procedures have been developed by NSA. The SABI process is an example of a procedure which should be adopted by the DoD and applied to the DON (and other services uniformly).



Strategy and Recommendations

The above chart provides the strategy and associated recommendations provided by the Panel.

A major assumption of the study, which was reinforced through all of the findings, is the fundamental tenet that national information must be protected. As an example, this is the major obstacle to sharing the SIPRNET with NATO. Allied and coalition partners. The present systems have no agreed upon means of partitioning access. FVE technology with high assurance guard provides allow secure, highly reliable systems which protect individual data for national participants within the context of managed risk. Recognizing that DON and national policies are not yet ready to restructure US classified nets, including SIPRNET, for partitioned access on need-to-know basis for Allied and coalition nations, the VOW concept would meet the mission informational needs of the operational participants while protecting security.

The technology to support the use of FVE is maturing. Adoption of developments in industry and DoD/NSA in this area should provide both the infrastructure and the necessary level of security for military systems. Continued investment should be made in high assurance guard systems, incorporating the technologies already demonstrated and used by DISA.

Strategy

- Demand interoperability in acquisition/training process

Recommendations

- 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
- CINCs promote international exercises/training and OPNAV/MCCDC ensure feedback to the acquisition system
- ASD(C4ISR)/DISA enforce interoperability and certification requirements

Strategy and Recommendations

The above chart provides the strategy and associated recommendations provided by the Panel.

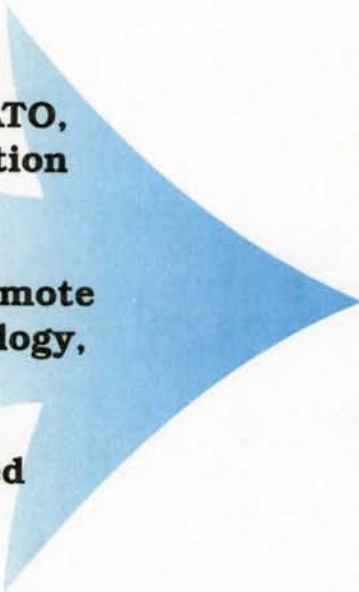
The DON is making huge strides in embracing and incorporating IT into every aspect of Navy and Marine Corps Force operations and has major initiatives, such as IT-21, underway to provide continuous progress. As a matter of course, incorporation of the hardware and software enabled by the technology has a strong focus for integration into legacy platforms and systems, as well as into emerging platforms. In practice, however, focus on delivery and performance of the new equipment, and integration details within the platform override interoperability considerations. This problem is exacerbated by incorporation of COTS without a carefully implemented interoperability plan. While both DoD and DON instructions call for attention to interoperability standards and certification at the Joint, NATO and Allied levels, such attention is often directed either too late in the development process or is applied when problems occur during fielding and deployment. Certification requirements are often waived, and upgrades for legacy platforms (beyond Milestone III) often bypass the instructions.

The Panel believes that interoperability issues must be addressed during the requirements process, i.e., during development of the

Operational Requirements Documents (ORD). The Panel further believes that interoperability certification needs to be more tightly linked with the acquisition process for system block upgrades as well as for new systems. Finally, the Panel notes that responsibility, authority, and accountability within the acquisition structure need to be addressed specifically for interoperability issues.

The Panel made these specific recommendations:

- Assign a specific acquisition interoperability oversight function within the Navy's and Marine Corps' acquisition community, whether it be within ASN(RD&A), DASN(C⁴I)/CIO, or a Program Executive Office (PEO) for interoperability. Such oversight must be extended to systems upgrades prior to approval for fielding. Additionally, all PEOs must be incentivized to achieve interoperability goals.
- Integrate planning for DT&E, OT&E, and interoperability certification tests, and satisfactorily complete testing in accordance with these integrated plans prior to fielding either new systems or upgrades.
- Pursuant to early interoperability requirements, the Panel recommends that a matrix of information interoperability needs/requirements be established, maintained and validated based upon demographics (theater) and levels (from OOTW to Major Regional Conflict (MRC)) of potential operations, levels of combatants and support groups.
- Construct a formal implementation plan for information systems and subsystems interoperability based upon minimum essential needs for information flow to a range of NATO, Allied and coalition forces for the anticipated range and level of fleet operations.
- Modify the acquisition process to assure approval (e.g. by the oversight function above) of an information interoperability plan at each milestone for new systems, and prior to approval for fleet incorporation of information system upgrades. The Panel found that "uncontrolled" system upgrades was a major source of interoperability problems. Further, such upgrades must not be pursued on a piecemeal basis.
- Formally educate and train the information systems acquisition workforce for specific issues surrounding interoperability, including lessons learned from prior systems interoperability issues. This training should be augmented by subject matter experts from the Fleet.
- With regard to operational training and the development of subject matter experts, the Panel recommends foreign exchange tours as an appropriate mechanism to gain insight relevant to allied and coalition interoperability issues.

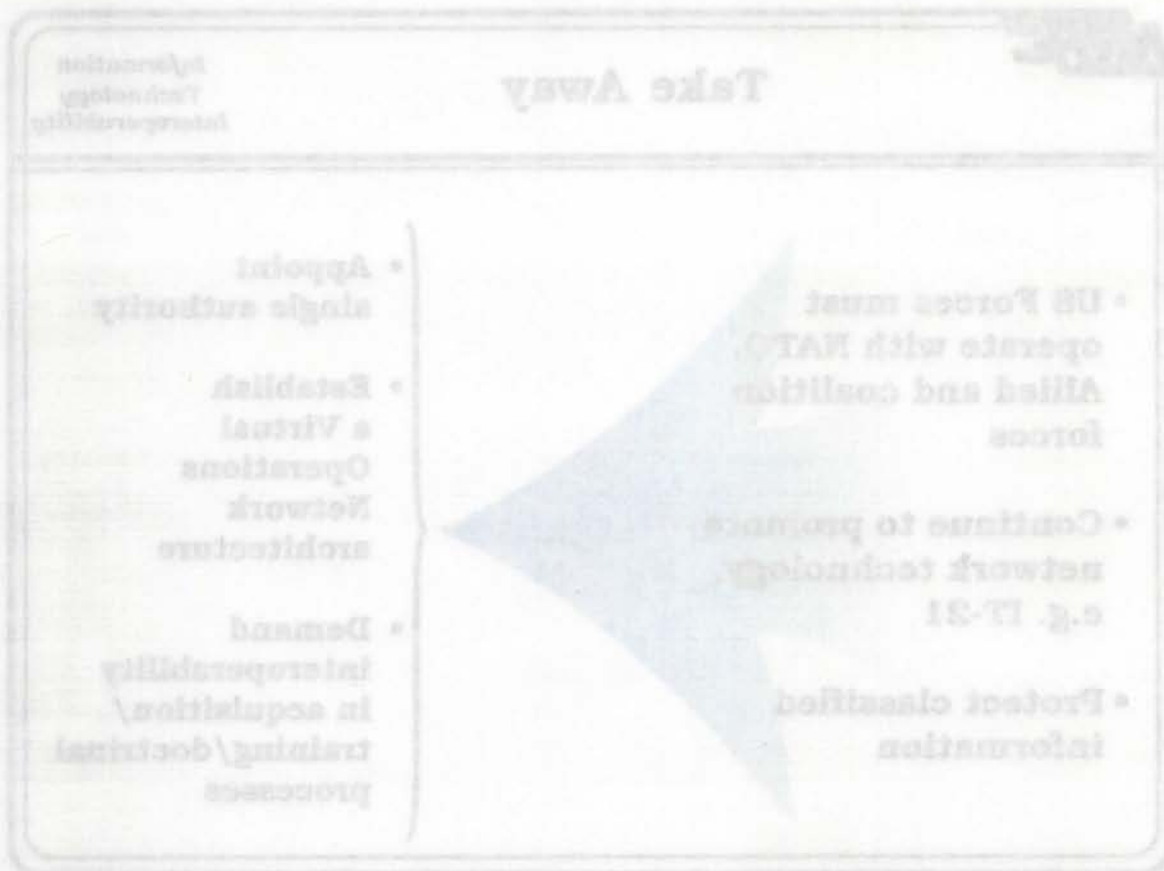
- 
- **US Forces must operate with NATO, Allied and coalition forces**
 - **Continue to promote network technology, e.g. IT-21**
 - **Protect classified information**
- **Appoint single authority**
 - **Establish a Virtual Operations Network architecture**
 - **Demand interoperability in acquisition/training/doctrinal processes**

Take Away

The US Navy and US Marine Corps need to focus their efforts to increase interoperability with NATO, Allied and coalition forces. In order to address broad IT interoperability requirements and solutions, DON should recommend that the Secretary of Defense (SECDEF)/CJCS designate a single US authority for interoperability with NATO, Allied and coalition forces. This authority should coordinate across joint, NATO, Allied and potential coalition partners. An authority should also be established within the DON to address interoperability issues.

To achieve a minimum capability to communicate with all of our partners, creation of a VON is recommended. The DON should invest in enabling technologies to achieve VON capabilities. Additionally, the DON should establish minimum equipment sets to provide to coalition partners who lack capability.

Finally, DON should consider modifications in its acquisition process to demand interoperability requirements. Currently the acquisition system and processes are incentivized in areas other than achieving IT interoperability.



Take Away

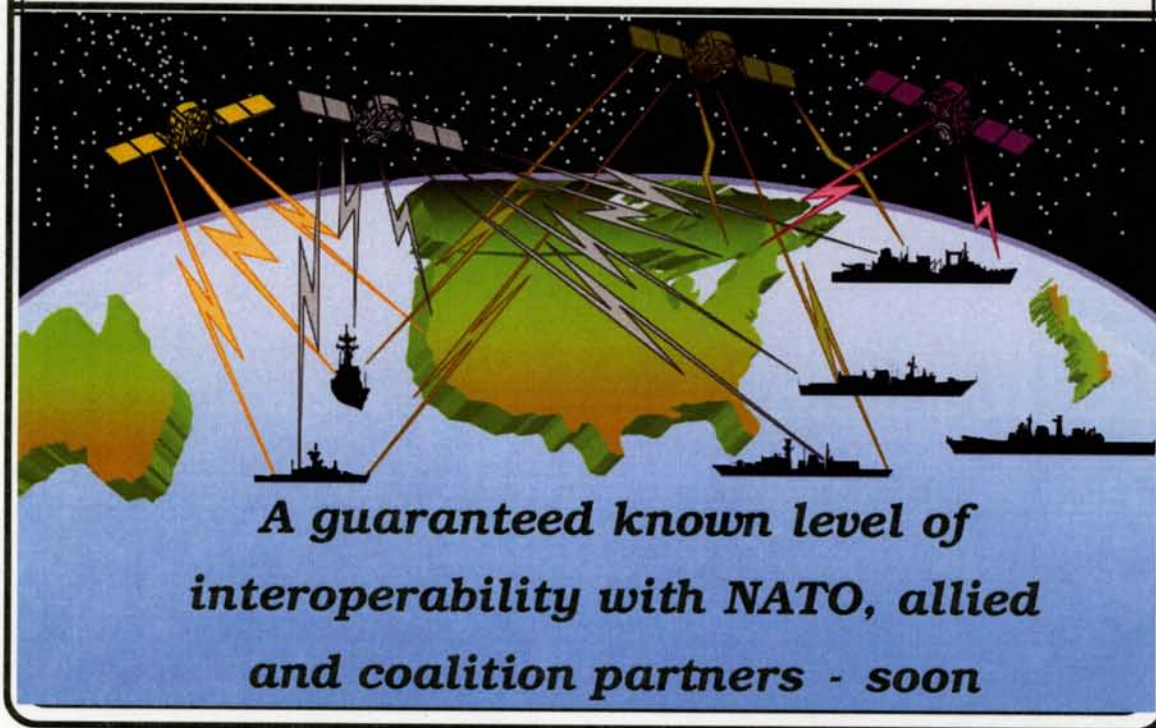
The US Navy and US Marine Corps need to focus their efforts to increase interoperability with NATO, Allied and coalition forces. In order to address broad IT interoperability requirements and solutions, DON should recommend that the Secretary of Defense (SECDEF)/OCS designates a single US authority for interoperability with NATO, Allied and coalition forces. This authority should coordinate across joint, NATO, Allied and potential coalition partners. An authority should also be established within the DON to address interoperability issues.

To achieve a minimum capability to communicate with all of our partners, creation of a VON is recommended. The DON should invest in enabling technologies to achieve VON capabilities. Additionally, the DON should establish minimum equipment sets to provide to coalition partners who lack capability.

Finally, DON should consider modifications in its acquisition process to demand interoperability requirements. Currently the acquisition system and processes are incentivized in areas other than achieving IT interoperability.

The Opportunity

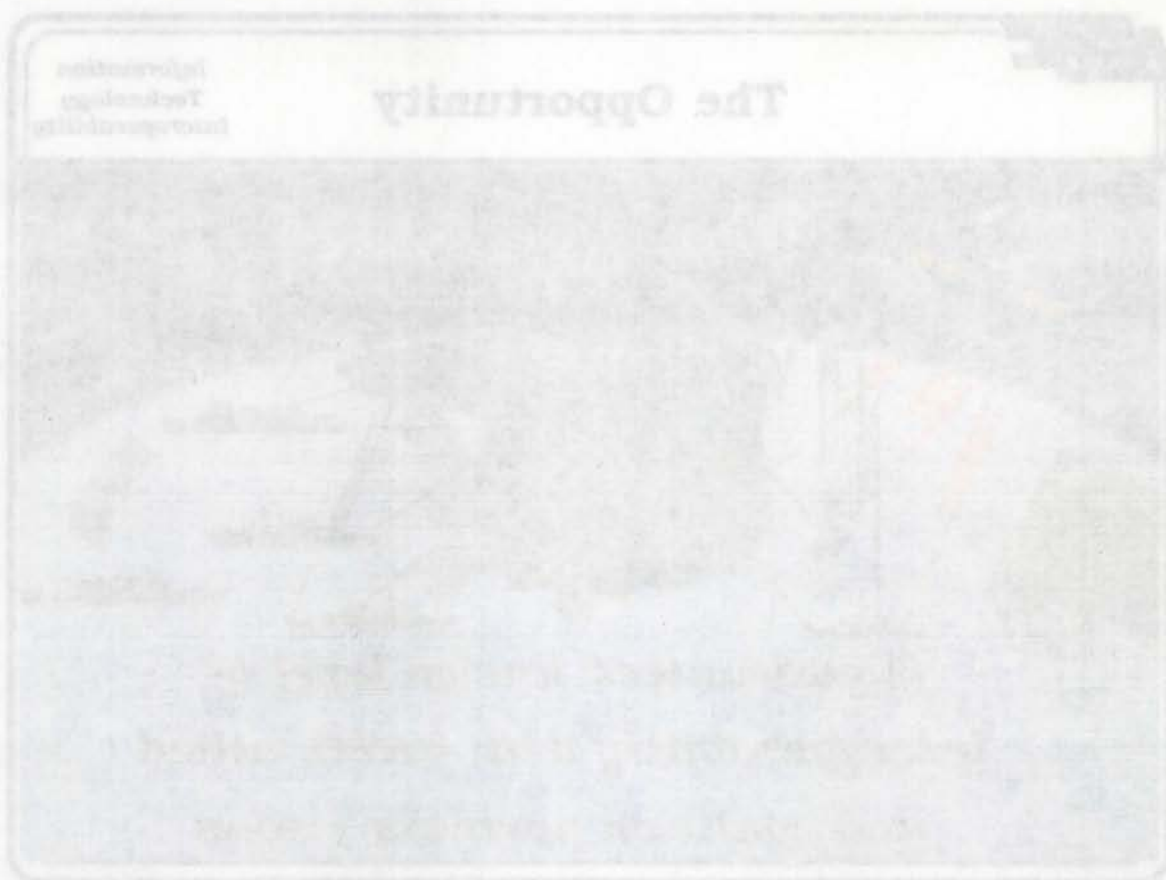
Information
Technology
Interoperability



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!



The Opportunity

If the DOD focuses on the Key Take Aways - 1) Appoint Single Authority; 2) Establish a VON architecture; 3) Demand interoperability in acquisition/training/doctoral 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.

APPENDIX A

BRIEFINGS/PANEL DISCUSSIONS/VIDEO TELECONFERENCES/VISITS

<u>Briefing Topic</u>	<u>Briefer</u>	<u>Title/Organization</u>
Network Centric Warfare	CAPT Gary Barrett, USN	Assistant for Strategic Planning (OPNAV N6C)
IT-21 Overview	RADM Richard W. Mayo, USN	Director, Allied and Fleet Requirements (OPNAV N60)
ONR Technologies for NATO	Dr. Sherman Gee	Communications Program Officer, Office of Naval Research
Sixth Fleet Operational Issues	Mr. Gary Toth	Sixth Fleet Science Advisor
USN Interoperability with High Tech Foreign Navies	Dr. Robert O'Dell	Center for Naval Analyses
Counter Transnational Threat	Dr. Robert Douglass	Assistant Director Integrated Infrastructure DARPA ISO
CINCUSNAVEUR Interoperability Assessment	LT Rick McCartney, USN	N6 Interoperability Officer CINCUSNAVEUR
Achieving C ⁴ I Interoperability in an era of Technological Innovation	CAPT P. R. Davies, CBE, RN	Directorate Communications and Information Systems (Navy)/AD(C ⁴ I), UK Ministry of Defence
COMUSNAVCENT C ⁴ I Progress for the 21 st Century	CAPT Dave Gelenter, USN	Assistant Chief of Staff for C ² W/IW/C ⁴ I (N6) COMUSNAVCENT
DERA briefs on STANAGS, Secondary Imagery Interoperability, UK Intelligence CIS Architecture, UK ASTOR program	Peter Doran, Mike Burstow, Tony Branton, Martin Smith, Dave Wallbank, John Beattie	
SHAPE brief	CDR Eric Randall, USN	Exercise Coordinator, SHAPE CIS Information Systems Branch
COMSECONDFLT issues	VADM William J. Fallon, USN CAPT Richard Stringer, USN	COMSECONDFLT/Commander Striking Force Atlantic ACOS COMSECONDFLT
Strong Resolve 98 overview	CDR Matthew Scassero, USN	NATO Exercise Officer Commander, Striking Force Atlantic
COMSECONDFLT C ⁴ I Overview	CDR Neal Miller, USN	ACOS for Communications and C ⁴ I Systems (J6), COMSECONDFLT
COMSECONDFLT Operational Requirements Overview	CDR Kevin Peppe, USN	COMSECONDFLT N3 staff
COMSECONDFLT Intelligence Overview	CAPT Thomas Dove, USN	ACOS for Intelligence (J2) COMSECONDFLT
IREN Virtual Lab	Mr. Jim Harper	Booz, Allen, and Hamilton

APPENDIX A (Continued) **BRIEFINGS/PANEL DISCUSSIONS/VIDEOTELECONFERENCES/VISITS**

<u>Briefing Topic</u>	<u>Briefer</u>	<u>Title/Organization</u>
Database/Information Technology	Mr. Walker White	Oracle
Cooperative Engagement Capability	Mr. Wayne Cantrell Mr. Conrad Grant	Director of CEC Programs, Raytheon Systems Communications Division Johns Hopkins University/Applied Physics Laboratory
Global Broadcast System/ Information Dissemination Management	Mr. D. Ahern	General Dynamics/Information Systems
Multi-level Information System Security	Mr. Greg Elkmann Mr. Gary Tater	NSA NSA Office of Security Management
NSA Interoperability Issues	LTCOL Mark Loeper, USA	Chief, Military Requirements Analysis Branch, Warfighter Information Security Support Division, Office of Customer Support Services National Security Agency
Defense Message System	Mr. Glenn Kurowski	Lockheed-Martin
Project Rainbow Brief	Dr. David Weisman	Technical Director, Project Rainbow, Lockheed-Martin
Trends in Telecommunications -The Next Century	Mr. Michael J. Geller	Lucent Technologies Government Solutions
C ⁴ I Technology Transfer	Mr. Gregg Bergersen	EW/C ⁴ I Policy Coordinator Navy International Program Office
Technology Challenges - IT-21	ADM Archie Clemens, USN	CINCPACFLT
Joint Interoperability Engineering Organization	Dr. Frank Perry	DISA Technical Director for Joint Interoperability and Engineering Organization, Technical Director for Engineering and Interoperability
Radiant Mercury Brief	MAJ Laura Bunker, USAF	National Reconnaissance Office
Radiant Mercury Releasability And Security Brief	LTCOL Enrique G. Hernandez, USAF	Director, International Program Office, National Reconnaissance Office
Extending the Littoral Battlespace ACTD	Dr. Tom Bordley	General Dynamics Advanced Technology Systems
Joint Staff Interoperability Perspective	CDR Tim Hanley, USN	Joint Staff, J6U

APPENDIX A (Continued)

BRIEFINGS/PANEL DISCUSSIONS/VIDEOTELECONFERENCES/VISITS

<u>Briefing Topic</u>	<u>Briefer</u>	<u>Title/Organization</u>
Phased Array Antenna	Mr. Geoffrey White	Boeing
Joint Continuous Strike Environment ACTD	Ms. Rosanne Hynes	Demonstration Manager, OSD/CISA
Link 16 ACTD	LTCOL Marty Meyer, USAF	USD(AT) staff
NRL Technology Initiatives	Dr. Glenn Cooper	
Marine Corps Perspective	COL Nick Hoffer, USMC	I MEF, G6
Globalstar and DoD Gateways	Mr. Mike Lapadula	QUALCOMM
The Naval Center for Tactical Systems Interoperability Command Brief and Issues	CAPT J.B. Gregor, USN Mr. Mike Gregory Mr. Pete Whidby	Commanding Officer, NCTSI Technical Director, NCTSI Global C ⁴ I Department Head, NCTSI
Navy Satellite Communications	CAPT James W. Loisele, USN CDR Neil C. Butler, USN LCDR Greg A. Hammond, USN	Program Manager APM Operations APM Acquisition Engineer Communication Satellite Systems (PMW-146)
Satellite Bandwidth, Frequency, and Antenna Size	Mr. Brian Colvin	Program Director JCOMMS Integration System (PMW-176-1)
Satellite Vulnerabilities	Mr. Brian Andersen	D841, SPAWAR System Center San Diego
Information Superiority	CAPT Dan Galick, USN	Program Manager, Information System Security/ Information Warfare - Defensive (IW-D) (PMW-161)
<u>Panel Discussion Topic</u>	<u>Participants</u>	
SHAPE Operations/Issues	CAPT Fitzgerald, USN Commodore Heath, CN	
SACLANT Interoperability Perspective	ADM Harold Gehman, USN CAPT Lewis, USN CAPT Holt, USN	USACOM/SACLANT
Naval Science Advisors-Problems and Limitations Working with Coalition Partners	Susan Bales Chris Vogt Gary Toth Ollie Allen Barry Podolsky Shane Deichman Sunny Cornwell Rich Hess	Director, Naval Science Advisor Program COMUSNAVCENT COMSIXTHFLT COMSEVENTHFLT COMTHIRDFLT COMMARFORPAC COMMARFORLANT CINCPACFLT

APPENDIX A (Continued)
BRIEFINGS/PANEL
DISCUSSIONS/VIDEOTELECONFERENCES/VISITS

<u>Videoteleconference Topic</u>	<u>Participants</u>	<u>Title/Organization</u>
Network Centric Warfare/IT-21	CAPT Traverso, USN	CINCPACFLT N6
Information Technology Issues	RADM John A. Gauss, USN	Commander, Space and Naval Warfare Systems Command
<u>Teleconference Topic</u>	<u>Participants</u>	
NAVCENT operations/issues	CAPT Dave Gelenter, USN	ACOS for C ² W/TW/C ⁴ I (N6) COMUSNAVCENT

Visits

Office of Naval Research, Arlington VA
 UK Ministry of Defence, London, UK
 UK Defence Evaluation and Research Agency, Malvern UK
 Supreme Headquarters Allied Powers Europe, Brussels, Belgium
 Commander Second Fleet Headquarters, Norfolk, VA
 Naval Research Lab, Washington DC
 MEFEX 98-1, Camp Pendleton, CA

JWID 98, SPAWAR Systems Center, San Diego, CA

APPENDIX B

Terms of Reference Naval Research Advisory Committee (NRAC) Panel on Assessing Information Technology (IT) Interoperability Among Systems, with a Focus on Coalition Warfare

General Objective: Assess technologies and interoperability implications associated with information transfer and interaction among systems as well as between systems, especially among and between NATO and coalition forces.

Background: There is a revolution occurring in the manner in which Naval Forces conduct operations based on the explosion of commercial information technologies. The revolution is the exploitation of technologies to establish information dominance and the conduct of network centric warfare. Many issues arise as it relates to interoperability among and between NATO and coalition forces. Primary areas of concern are interoperability with legacy systems (e.g., communications, message formats, hardware and software applications, and language translation).

Specific Tasking:

1. Identify interoperability obstacles among and between command, control, communications, computers, intelligence surveillance and reconnaissance systems (C⁴ISR)/Combat Systems relative to joint, NATO and coalition Naval Forces.
2. Evaluate current and envisioned plans and procedures for mitigating adverse effects of rapidly moving technology.
3. Provide an assessment of existing and near-term technologies that will enable secure interoperability among and between essential systems.
4. Recommend a Department of the Navy strategy that achieves and maintains levels of interoperability required to support execution of Naval missions in a joint/NATO/coalition force environment.

Study Sponsor: VADM Arthur Cebrowski, USN, Director, Space, Information Warfare, Command and Control (N6), OPNAV.

APPENDIX B

Terms of Reference Naval Research Advisory Committee (NRAC) Panel on Assessing Information Technology (IT) Interoperability Among Systems With a Focus on Coalition Warfare

General Objective: Assess technologies and interoperability implications associated with information transfer and interaction among systems as well as between systems, especially among and between NATO and coalition forces.

Background: There is a revolution occurring in the manner in which naval forces conduct operations based on the explosion of commercial information technologies. The revolution is the explosion of technologies to establish information dominance and the conduct of network warfare. Many issues arise as it relates to interoperability among and between NATO and coalition forces. Primary areas of concern are interoperability with legacy systems (e.g., communications, message formats, hardware and software applications, and language translation).

Specific Tasks:

1. Identify interoperability obstacles among and between command, control, communications, computers, intelligence surveillance and reconnaissance systems (C4ISR) systems relative to joint, NATO and coalition Naval Forces.
2. Evaluate current and envisioned plans and procedures for mitigating adverse effects of rapidly moving technology.
3. Provide an assessment of existing and near-term technologies that will create secure interoperability among and between essential systems.
4. Recommend a Department of the Navy strategy that achieves and maintains levels of interoperability required to support execution of Naval missions in a joint/NATO/coalition force environment.

Study Sponsor: VADM Arthur Colwell, USN, Director, Space Information Warfare, Command and Control (SW/OPNAV).

APPENDIX C

Program, Concept, and System Descriptions

Base-Level Information Infrastructure (BLII)

BLII provides the Navy and Marine Corps sustaining base connectivity to the Defense Information Systems Network (DISN). It will modernize shore-based switches and cable plants and shipboard LANS to facilitate seamless connectivity and information flow.

Battle Group Passive Horizon Extension System - Surface Terminal (BGPHERS-ST)

BGPHERS-ST extends the battle group's line-of-site radio horizon and enhances joint interoperability by controlling remote sensors in an aircraft's sensor payload to relay radio transmissions to the ship's surface terminal via the Common High Bandwidth Data Link (CHBDL). The primary aircraft employed for this task is the Navy's ES-3A Viking; additionally, BGPHERS will be interoperable with the Air Force's U-2 reconnaissance aircraft.

Common High Bandwidth Data Link - Shipboard Terminal (CHBDL-ST)

CHBDL-ST provides a common data terminal for the receipt of signal and intelligence data from remote sensors and the transmission of link and sensor control data to airborne platforms. CHBDL-ST will interface with shipboard processors of the Joint Services Imagery Processing System-Navy (JSIPS-N) and the BGPHERS-ST. CHBDL-ST will process link data from BGPHERS or Advanced Tactical Airborne Reconnaissance (ATAR) aircraft configured with modular interoperability data link terminals.

Command Support System (CSS)

UK Navy equivalent of GCCS. It is a comprehensive, automated, C² tool. It eliminates confusion by providing: (1) force-wide, Common Operational Picture, (2) rapid, error-free information transfer, and (3) unequivocal application of doctrine. CSS is required to be compatible with the US Navy Joint Maritime Command Information System (JMCIS)/GCCS-Maritime.

Common Tactical Picture (CTP)

The knowledge and situational awareness that enhances combat identification, force coordination, and command and control. Associated programs include: GCCS which is the single most important C² initiative in the joint arena today.

APPENDIX C (Continued)

Crisis Response Operations in NATO Open Systems (CRONOS)

Concept developed to provide: (1) compatible LAN's at various levels of NATO command; (2) a fast resilient wide area network (WAN); (3) allow for technical evolution; and (4) a fully secure and accredited system.

Defense Message System (DMS)

The DMS offers secure, accountable, and reliable writer-to-reader messaging services at a reduced cost. The DMS consists of all hardware, software, procedures, standards, personnel and facilities required to exchange electronic messages between organizations. The common messaging environment offered by the DMS is designed to be flexible and interoperable between the Military Services, DoD agencies, and our NATO, Allied and coalition partners.

Enterprise Solutions

Involves the sharing of critical data in real-time across the enterprise organizations. Enterprise solutions must be developed through system-of-systems design. It goes beyond wire, cables, and routers.

Global Command and Control System (GCCS)

GCCS – is a modern C⁴ system which incorporates the core planning and assessment tools required by combat commanders for a fused picture of the battlespace. GCCS was developed as a COEThan to ensure improved system performance and interoperability.

Information Dissemination Management (IDM)

IDM optimizes information funds for the dissemination of information from sources to users, in accordance with the commander's information dissemination policy and user's name. Uses the GBS as the communications and transmission medium for large volume information and imagery.

Information Exchange Memoranda (IEM) include:

Military Information Exchange Memoranda (MIEM)

Military Multi-lateral Information Exchange Memoranda (MMIEM)

Information Exchange Programs (IEP's)

Technology Research and Demonstration Programs (TRDP's)

APPENDIX C (Continued)

IEM's are a means of exchanging/sharing information on current systems and future developments to promote convergent development and avoid divergent procurement. Agreements may be bi-lateral or multi-lateral and generally focus on one area of technology or warfare field (i.e. software intensive systems, gun/missile technology, active sonar, and fiber optic technology).

Information Technology for the 21st Century (IT-21)

The IT-21 goal is to enable voice and video transmission from a single desktop PC, which would enable the warfighter to exchange classified and unclassified tactical support information from the same workstation. It is envisioned to use browser technology, with continuous TCP/IP connections and multi-level security, in a client-server environment.

Integrated Broadcast Service (IBS)

The goal of the IBS is to resolve the uncoordinated proliferation of "stovepipe" intelligence broadcasts by providing the tactical commander with an integrated time-sensitive tactical intelligence information.

Joint Maritime Command Information System (JMCIS) 98

JMCIS is the core program of the Navy and Marine Corps' part of the GCCS. JMCIS combines numerous programs to provide the warfighter a common tactical picture on a common workstation. JMCIS provides timely, accurate, and complete all-source C⁴ISR information management, display, and dissemination capability for warfare mission assessment, planning, and execution. JMCIS is compliant with the Defense Information Infrastructure Common Operating Environment and incorporates the Marine Air Ground Task Force (MAGTF) C⁴I software baseline.

Multi/functional Information Distribution System (MIDS)

MIDS is being developed as an alternative to the Joint Tactical Information Distribution System (JTIDS). It is primarily being designed for aircraft and thus will be packaged in a smaller configuration.

Radiant Mercury

Radiant Mercury provides automated sanitization of data from Sensitive Compartmented Information (SCI) to General Service (GENSER). It allows/provides the ability to share sensitive data with our NATO, allied and coalition partners while protecting the data source.

APPENDIX C (Continued)

Tactical Common Info Management System (TACCIMS)

Korean Network which has been interfaced to SIPRNET during exercises, allows authorized transfer of data at approved levels.

Tactical Digital Information Link J (TADIL J) (NATO designation = LINK 16J)

A follow on to LINK 4A/11, it does not significantly change the basic concepts of tactical data link information exchange. LINK 16 does provide certain technical and operational improvements that include: jam resistance; improved security; and increased data rate (throughput). TADIL J/LINK 16 uses the Joint Tactical Information Distribution System (JTIDS) as it's communication component.

APPENDIX D

ABCA	American, British, Canadian Australian Armies Standardization Program
ACOM	Atlantic Command
ACTD	Advanced Concept Technology Demonstration
ADSIA	Allied Data System Interoperability Agency
ADSN	Advanced Digital Network System
ASCC	Air Standardization Coordinating Committee
ASD(C ⁴ ISR)	Assistant Secretary of Defense for C ⁴ ISR
ASN(RD&A)	Assistant Secretary of the Navy (Research, Development and Acquisition)
ATAR	Advanced Tactical Airborne Reconnaissance
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Order
ATP-1	Allied Tactical Publications 1
AUSCANNZUKUS	Australia-Canada-New Zealand-United Kingdom-United States Naval Command, Control, and Communications Organization
BADD/IDM	Battlefield Awareness Data Dissemination/Information Data Management
BAM	Bandwidth Assessment Memorandum
BGPHERS-ST	Battle Group Passive Horizon Extension System-Surface Terminal
BLII	Base-Level Information Infrastructure
C ²	Command and Control
C ² G	Command and Control Guard
C ³	Command, Control, and Communications
C ³ I	Command, Control, Communications and Intelligence
C ⁴ I	Command, Control, Communication, Computers, & Intelligence
C ⁴ ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CARAT	Cooperation Afloat Readiness and Training
CCB	Configuration Control Board
CCEB	Combined Communications-Electronics Board
CCIB	C ² Interoperability Boards
CDMA	Code Division Multiple Access
CEC	Cooperative Engagement Capability
CEO	Chief Executive Officer
CG	Commanding General

APPENDIX D (Continued)

CHBDL	Common High Bandwidth Data Link
CHBDL-ST	Common High Bandwidth Data Link - Shipboard Terminal
CINC	Commanders in Chief
CINCLANTFLT	Commander in Chief, US Atlantic Fleet
CINCPACFLT	Commander in Chief, US Pacific Fleet
CINCUSACOM	Commander in Chief, US Atlantic Command
CINCUSNAVEUR	Commander in Chief, US Naval Forces Europe
CIO	Chief Information Officer
CIS	Communications and Information Systems
CJCS	Chairman of the Joint Chiefs of Staff
COMMARFORLANT	Commander Marine Forces Atlantic
COMMARFORPAC	Commander Marine Forces Pacific
COMSIXTHFLT	Commander SIXTH Fleet
COMSECONDFLT	Commander SECOND Fleet
COMSEVENTHFLT	Commander SEVENTH Fleet
COMUSNAVCENT	Commander, US Naval Forces, Central Command
CNA	Center for Naval Analyses
CNO	Chief of Naval Operations
CNSI	Communications Systems Networking Interoperability
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CRONOS	Crisis Response Operations in NATO Open System
CSNI	Communications Systems Network Interoperability
CSS	Command Support System
CTP	Common Tactical Picture
DARPA	Defense Advanced Research Projects Agency
DASN	Deputy Assistant Secretary of the Navy
DASN(C ⁴ I)	Deputy Assistant Secretary of the Navy for Command, Control, Communications, Computers and Intelligence
DCIS	Directorate Communications and Information Systems
DERA	Defence Evaluation and Research Agency (UK)
DII/COE	Defense Information Infrastructure/ Common Operation Environment
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DISP	Directory Internet Services Provider
DMS	Defense Message System

APPENDIX D (Continued)

DoD	Department of Defense
DODIIS	Department of Defense Intelligence Information System
DON	Department of the Navy
DSA	Directory Service Agents
DSCS	Defense Satellite Communication System
DT&E	Development, Test and Evaluation
ELB	Extending Littoral Battlespace
FBE	Fleet Battle Experiment
FNBDT	Future Narrow Band Digital Terminal
FORTEZZA	Cryptographic Device Containing US Government Algorithms
FTP	File Transfer Protocol
GAO	Government Accounting Office
GBS	Global Broadcast System
GCCS	Global Command & Control System
GCCS-M	Global Command & Control System - Maritime
GCSS	Global Combat Support System
GENSER	General Service
GPS	Global Positioning System
GSM	Ground Station Module
HF	High Frequency
html	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
IBS	Integrated Broadcast Service
IDM	Information Dissemination Management
IEM	Information Exchange Memoranda
IEP	Information Exchange Program
IIP	Interoperability Improvement Panel
IMB	Interoperability Management Board
IO	Interoperability Objectives
IT	Information Technology
IT-21	Information Technology for the 21 st Century
ITI	Information Technology Interoperability
ITP	Interoperability Test Panel
IW	Information Warfare
IW-D	Information Warfare-Defense
JBC	Joint Battle Center
JCS	Joint Chiefs of Staff

APPENDIX D (Continued)

JC ² WC	Joint Command and Control Warfare Center
JCSE	Joint Continuous Strike Environment
JIEO	Joint Interoperability Engineering Organization
JITC	Joint Interoperability Test Center
JMCIS	Joint Maritime Command Information System
JMCOMM	
JMTSWG	Joint Multi-TADIL Standards Working Group
JP	Joint Publication
JSIPS-N	Joint Services Imagery Processing System-Navy
JTA	Joint Technical Architecture
JTFEX	Joint Task Force Exercise
JTIDS	Joint Tactical Information Distribution System
JVMF	Joint Variable Message Format
JWFC	Joint Warfighting Center
JWICS	Joint Worldwide Intelligence Communications Systems
JWID	Joint Warfare Interoperability Demonstration
Kbps	Kilobits Per Second
LAN	Local Area Network
LAN	LAN Emulation
LEOS	Low Earth Orbiting Satellite
LOCE	Linked Operational Intelligence Centers Europe
MAGTF	Marine Air Ground Task Force
MAIS	Major Automated Information System
MAS	Military Agency for Standardization
Mbps	Megabits Per Second
MCCDC	Marine Corps Combat Development Command
MCEB	Military Communications Electronics Board
MCTSSA	Marine Corps Tactical Systems Support Activity
MDAP	Major Defense Acquisition Programs
MEF	Marine Expeditionary Force
MIDS	Multi-Functional Information Distribution System
MIEM	Military Information Exchange Memoranda
MMIEM	Military Multi-Lateral Information Exchange Memoranda
MRC	Major Regional Conflict
NATO	North Atlantic Treaty Organization

APPENDIX D (Continued)

NAVCENT	Naval Forces, US Central Command
NCTSI	Navy Center For Tactical System Interoperability
NIPRNET	Unclassified but Sensitive (N-Level) Internet Protocol Router Network
NRAC	Naval Research Advisory Committee
NRL	Naval Research Laboratory
NSA	National Security Agency
NT	Personal Computer Operating System
O & M	Operations and Maintenance
OIRG	Operations Interoperability Requirements Group
ONR	Office of Naval Research
OOTW	Operations Other Than War
OPNAV	Office of the Chief of Naval Operations
OR (Sea)	Operational Requirements (Sea)
ORD	Operational Requirements Document
OSD	Office of the Secretary of Defense
OT&E	Operational Test and Evaluation
PARP	Planning and Review Process
PC	Personal Computer
PEO	Program Executive Office
PfP	Partners for Peace
PfPEX	Partner for Peace Exercise
PKE	Public Key Encryption
PKI	Public Key Encryption Infrastructure
R & D	Research and Development
RD&A	Research, Development and Acquisition
RDA	Research Development and Acquisition
RIMP	Rim of the Pacific Exercise
SABI	Secret and Below Initiative
SACLANT	Supreme Allied Commander, Atlantic
SATCOM	Satellite Communications
SCI	Sensitive Compartmented Information
SECDEF	Secretary of Defense
SECONDFLT	Second Fleet
SHAPE	Supreme Headquarters Allied Powers Europe
SHF	Super High Frequency
SIPRNET	SECRET Internet Protocol Router Network
SMTF	Simple Mail Transfer Protocol
SNMP	System Network Management Protocol
SPAWAR	Space and Naval Warfare Systems Command

APPENDIX D (Continued)

SR-98	Strong Resolve Exercise 1998
STANAGS	Standardization Agreement (NATO)
SYSCOMS	Systems Commands
TACCIMS	Tactical Common Info Management System
TADIL	Tactical Digital Information Link
TCP/IP	Transport Control Protocol/Internet Protocol
THIRDFLT	Third Fleet
TISG	Technical Interoperability Standards Group
TOR	Terms of Reference
TPFD	Time Phased Force Deployment
TRDP	Technology Research and Demonstration Programs
UHF	Ultra High Frequency
UK	United Kingdom
UNIX	Work Station Operating System
US	United States
USACOM	United States Atlantic Command
USD(AT)	Under Secretary of Defense (Acquisition and Technology)
USN	United States Navy
VON	Virtual Operations Network
VTC	Video Teleconference
WAN	Wide Area Network
X.400	Industry E-mail standard
X.500	Industry directory standard
X.509	Industry security certificate standard