

UNCLASSIFIED

ACP 200(C) Vol 1

MARITIME TACTICAL WIDE AREA NETWORKING (MTWAN)

OPERATING INSTRUCTIONS



Uncontrolled copy when printed

ACP 200(C) Volume 1

March 2010

i

UNCLASSIFIED

FOREWORD

1. The Combined Communications-Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the Sponsoring Authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.
2. ACP 200(C) Volume 1, MARITIME WIDE AREA TACTICAL NETWORKING (MTWAN) Operating Instructions, is an UNCLASSIFIED CCEB publication.
3. This publication contains Allied military information for official purposes only.
4. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP 198.

Uncontrolled copy when printed

**THE COMBINED COMMUNICATIONS-ELECTRONICS BOARD LETTER OF PROMULGATION
FOR ACP 200(C) Volume 1**

1. The purpose of this Combined Communications-Electronics Board (CCEB) Letter of Promulgation is to implement ACP 200(C) Volume 1 within the Armed Forces of the CCEB Nations. ACP 200(C) Volume 1, MARITIME WIDE AREA NETWORKING (MTWAN) Operating Instructions, is an UNCLASSIFIED publication developed for Allied use under the direction of the CCEB Principals
2. ACP 200(C) Volume 1 is effective upon receipt for CCEB Nations and when directed by the NATO Military Committee (NAMILCOM) for NATO nations. ACP 200(C) Volume 1 and Volume 2 will supersede ACP 200(C), which shall be destroyed in accordance with national regulations.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 200(C) Vol 1	CCEB	On Receipt	LOP

3. All proposed amendments to the publication are to be forwarded to the national coordinating authorities of the CCEB or NAMILCOM.

For the CCEB Principals

Paul Foster
P. FOSTER
Major, CF
CCEB Permanent Secretary

Uncontrolled copy when printed

TABLE OF CONTENTS

FOREWORD	ii
THE COMBINED COMMUNICATIONS-ELECTRONICS BOARD LETTER OF PROMULGATION	iii
RECORD OF MESSAGE CORRECTIONS	iv
TABLE OF CONTENTS	v
LIST OF FIGURES.....	ix
LIST OF TABLES.....	x
CHAPTER 1	1-1
INTRODUCTION.....	1-1
OVERVIEW.....	1-1
BACKGROUND.....	1-1
AIM	1-1
SCOPE.....	1-1
CAPABILITY.....	1-2
DOCUMENT STRUCTURE	1-3
CONCLUSION.....	1-4
CHAPTER 2	2-1
CONCEPT OF OPERATIONS.....	2-1
INTRODUCTION	2-1
AIM	2-1
SCOPE.....	2-1
OVERVIEW.....	2-1
OPERATIONAL VIEW	2-2
SYSTEMS VIEW.....	2-4
COMMUNICATIONS ARCHITECTURE.....	2-6
ROUTING ARCHITECTURE	2-7
SECURITY ARCHITECTURE	2-8
APPLICATIONS / INFORMATION TYPES	2-9
TECHNICAL VIEW	2-10
ROUTING.....	2-12
COMMUNICATION SUBNETS	2-12
TRANSPORT SERVICES	2-12
CONCLUSION.....	2-13
CHAPTER 3	3-1
INFORMATION MANAGEMENT (IM).....	3-1
INTRODUCTION	3-1
AIM	3-1
OVERVIEW.....	3-1
DEFINITION	3-3
PRINCIPLES	3-3
VALUE OF INFORMATION	3-4
IM CONSIDERATIONS	3-5
COMMAND AND CONTROL (C2) DECISION CYCLE.....	3-6
INFORMATION DISSEMINATION MANAGEMENT (IDM)	3-8
INFORMATION DISSEMINATION PLAN (IDP)	3-9
INFORMATION MANAGEMENT TOOLS	3-12
INFORMATION MANAGEMENT IMPEDIMENTS	3-12
MINIMIZE.....	3-15
OPSEC – RIVERCITY PROCEDURES	3-15
FILE NAMING CONVENTION	3-15
CONCLUSION	3-16

ANNEX A TO CHAPTER 3----- 3A-1
ANNEX B TO CHAPTER 3-----3B-1
ANNEX C TO CHAPTER 3-----3C-1
ANNEX D TO CHAPTER 3----- 3D-1

CHAPTER 4 4-1
SECURITY 4-1
INTRODUCTION -----4-1
AIM -----4-1
OVERVIEW-----4-1
DEFINITIONS -----4-1
REFERENCE-----4-2
NETWORK TOPOLOGY-----4-2
POINT OF PRESENCE / BOUNDARY PROTECTION DEVICES-----4-3
THREATS-----4-4
RESPONSIBILITIES -----4-5
EXPORT SANCTION -----4-5
ASSUMPTIONS -----4-6
RECOMMENDED SECURITY ARCHITECTURES -----4-6
NETWORK CONNECTIVITY -----4-6
SHIPBOARD “AIR GAP” ARCHITECTURE-----4-7
SHIPBOARD “NETWORKED” ARCHITECTURE-----4-8
SHIPBOARD “FULLY INTEGRATED” TARGET ARCHITECTURE. -----4-9
ACCREDITATION -----4-11
SECURITY DEVICE INTEROPERABILITY -----4-11

CHAPTER 5 5-1
TRAINING AND INTEROPERABILITY 5-1
INTRODUCTION -----5-1
AIM -----5-1
OVERVIEW -----5-1
TRAINING-----5-1
INTEROPERABILITY LEVEL-----5-1
DETERMINING INTEROPERABILITY LEVEL -----5-1
REPORTING PROCEDURES -----5-2

CHAPTER 6 6-1
MESSAGING 6-1
INTRODUCTION -----6-1
AIM -----6-1
OVERVIEW -----6-1
TYPES OF MESSAGING-----6-2
TEXT-BASED FORMATS -----6-2
CHAT -----6-2
MULTIMEDIA FORMATS -----6-2
E-MAIL-----6-3
WEB SERVICES -----6-3
MESSAGING SELECTION-----6-3
MULTICAST MESSAGING -----6-4
PUBLIC KEY INFRASTRUCTURE (PKI)-----6-7
CONCLUSION-----6-7
ANNEX A TO CHAPTER 6----- 6A-1

CHAPTER 7 7-1
COMMON OPERATIONAL PICTURE (COP)..... 7-1
INTRODUCTION -----7-1
AIM -----7-1

Uncontrolled copy when printed

OVERVIEW -----7-1

REQUIREMENT -----7-2

TOP COP (FUSION AND FILTERING)-----7-2

COP MANAGEMENT -----7-2

FOTC-----7-3

CST-----7-3

DUAL FOTC / CST -----7-3

COP DISSEMINATION -----7-3

CSTMDXNET / CST-----7-3

UNIT IDENTIFIER (UID)-----7-3

NETPREC-----7-3

MULTICAST TRANSPORT SERVICE -----7-4

COP ARCHITECTURE -----7-4

SELECTION OF APPROPRIATE COP DISSEMINATION METHOD-----7-5

CONCLUSION-----7-6

ANNEX A TO CHAPTER 7----- 7A-1

CHAPTER 8..... 8-1

WEB SERVICES 8-1

INTRODUCTION -----8-1

AIM -----8-1

OVERVIEW -----8-1

OBJECTIVE -----8-1

DEFINITIONS -----8-1

FUNCTIONAL DESCRIPTION -----8-2

WEB ADMINISTRATION -----8-4

WEB ADMINISTRATOR -----8-4

WEB DEVELOPER -----8-4

INFORMATION MANAGER -----8-4

Information Producers-----8-4

PRINCIPLES -----8-5

REQUIREMENTS-----8-5

CONNECTIVITY -----8-6

PERSISTENT CONNECTIVITY -----8-6

ONE-WAY REPLICATION -----8-6

BI-DIRECTIONAL REPLICATION -----8-6

TRANSACTION LOGGING -----8-6

WEB CONTENT / PAGES -----8-7

HOW USERS EXPERIENCE THE WEB-----8-7

USERS CHOICES -----8-7

RESPONSE TIMES -----8-7

WEB PAGE GUIDELINES -----8-8

SHORT TEXTS -----8-8

REVIEWING TEXT -----8-8

POSTING DOCUMENTS -----8-8

HIERARCHY OF INFORMATION -----8-9

WEB INTERFACES -----8-9

PORTAL -----8-9

TEMPLATES -----8-9

CONCLUSION-----8-10

ANNEX A TO CHAPTER 8----- 8A-1

ANNEX B TO CHAPTER 8-----8B-1

ANNEX C TO CHAPTER 8-----8C-1

CHAPTER 9..... 9-1

DISTRIBUTED COLLABORATIVE PLANNING 9-1

Uncontrolled copy when printed

INTRODUCTION -----9-1
AIM -----9-1
OVERVIEW -----9-2
IMPORTANCE -----9-2
TIMELINESS -----9-2
EFFECTIVENESS -----9-2
COLLABORATIVE PLANNING SPECTRUM -----9-2
AWARENESS -----9-3
CONVERSATION -----9-3
SHARED OBJECTS -----9-4
GLOBAL ADDRESS BOOK -----9-4
BLENDING ASYNCHRONOUS AND REAL-TIME COLLABORATION -----9-4
CONFIGURATION -----9-6
BANDWIDTH LIMITATIONS -----9-7
TOOLS -----9-7
REQUIREMENTS -----9-7
CONCLUSION -----9-7
ANNEX A TO CHAPTER 9 ----- 9A-1
ANNEX B TO CHAPTER 9 -----9B-1
ANNEX C TO CHAPTER 9 -----9C-1
GLOSSARY OF TERMS ----- Glossary-1
LIST OF EFFECTIVE PAGES -----LEP-1

Uncontrolled copy when printed

LIST OF FIGURES

Figure 1-1: Maritime Network Domains	1-2
Figure 1-2: Document Architecture	1-3
Figure 1-3: Document Structure	1-4
Figure 2-1: Determinants of Information Value	2-2
Figure 2-2: Operational View (OV-1)	2-3
Figure 2-3: Systems View (SV-1.1).....	2-4
Figure 2-4: Systems View (SV-1.2).....	2-5
Figure 2-5: Systems View (SV-1.3).....	2-7
Figure 2-6: Technical View (TV-1.1).....	2-9
Figure 2-7: Technical View (TV-1.2).....	2-10
Figure 3-1: IM Hierarchy.....	3-2
Figure 3-2: Determinants of Information Value	3-3
Figure 3-3: Impact of Presentation Form.....	3-4
Figure 3-4: C2 Decision Cycle	3-6
Figure 3-5: IDM.....	3-7
Figure 3-6: Example Battle Rhythm	3-9
Figure 3-7: Daily Operations Cycle	3-10
Figure 3-D-1: Fast Save	3D-2
Figure 3-D-2: Master Slides.....	3D-3
Figure 4-1: MTWAN Topology.....	4-2
Figure 4-2: Boundary Protection Devices Between Domains	4-3
Figure 4-3: MTWAN Connectivity	4-7
Figure 4-4: Air Gap Architecture.....	4-8
Figure 4-5: Networked Architecture	4-9
Figure 4-6: “Fully Integrated” Target Architecture	4-10
Figure 7-1: Traditional Environment (with IXS networks and CST).....	7-4
Figure 7-2: Full IP Environment (MTWAN).....	7-5
Figure 8-1: Service Orientated Architecture.....	8-4
Figure 8-A-1: Generic Replication Architecture	8A-2
Figure 8-A-2: Mesh Replication Architecture	8A-3
Figure 8-A-3: Federated Hub-Spoke Replication Architecture	8A-4
Figure 8-B-1: Typical Page Structure	8B-1
Figure 8-B-2: Global Area Content	8B-2
Figure 8-C-1: Software Building Block Reuse.....	8C-3
Figure 9-1: Collaborative Planning Spectrum	9-4
Figure 9-2: DCP Characteristics	9-5
Figure 9-3: DCP Configurations.....	9-6
Figure 9-B-1: Bandwidth Aggregation	9B-3
Figure 9-B-2: Operator Number Impact on Bandwidth.....	9B-5

LIST OF TABLES

Table 3-1: Information Dissemination Plan (IDP).....3-12
Table 3-A-1: OPTASK IM – Priority of Service (POS) Key3A-3
Table 3-A-2: OPTASK IM – Message Field Set3A-5
Table 5-1: WAN Link5-2
Table 5-2: Minimum Dedicated Bandwidth5-2
Table 5-3: Supported Applications5-2
Table 5-4: Interoperability Matrix5-3
Table 6-1: Messaging Selection.....6-6
Table 7-1: COP Dissemination Methods7-5
Table 7-A-1: Combined Requirements for COP7A-1
Table 8-1: Standards behind Web Services8-3
Table 9-1: DCP Spectrum.....9-3
Table 9-B-1: Bandwidth Toolset Spectrum9B-2
Table 9-C-1: Tactical Networking Command And Control Tools9C-1

Uncontrolled copy when printed

CHAPTER 1

INTRODUCTION

OVERVIEW

101. A Maritime Tactical Wide Area Network (MTWAN) is an affordable, effective and efficient means to share information in a tactical environment. This publication provides guidance as to the procedures, applications, infrastructure and data attributes required for tactical mobile IP networking. To enable widest distribution, the information contained within the main part of this document is unclassified. Classified information will be incorporated in separate supplements.

BACKGROUND

102. In the mid to late 1990s, Operational Commanders recognized that the existing procedures, applications, infrastructure, and data standards could not support Allied and Coalition Information Exchange Requirements (IER). Increased levels of formal message traffic resulted in message traffic backlogs, delays, and non-delivery. This was especially pertinent during periods of high intensity operations. Furthermore, the large amount of information could not be easily assimilated due to the way it was presented.

103. To address this issue a number of related initiatives were implemented. During Joint Warrior Interoperability Demonstration (JWID) 97 the initial aspects of a multi-national maritime WAN were demonstrated, and in RIMPAC 98 Commander Pacific Fleet (COMPACFLT) established what was to become a Wide Area Network (WAN) between Australia, Canada, United Kingdom, and the United States.

104. Subsequently, there have been many incremental advances driven by operational requirements that led to the creation of a number of tactical mobile WANs or the extension of shore-based networks to sea. AUSCANNZUKUS also continued refining doctrine and solutions through participation in laboratory and sea-based experimentation and feedback from the naval war fighter.

AIM

105. The aim of this publication is to provide guidance for the design, implementation, and operation of a MTWAN.

SCOPE

106. This publication is applicable to the operators and technicians who are responsible for the establishment, operation, and maintenance of a WAN in a mobile tactical environment. It is designed for use in conjunction with other operational documents and provides:

- a. An overarching document for current maritime networks;
- b. Guidance to the establishing a MTWAN; and

- c. A goal MTWAN architecture.

CAPABILITY

107. An MTWAN is a maritime Internet Protocol (IP) based network developed to promote the effective and efficient sharing of information within the maritime tactical environment. The term “MTWAN” used in the context of this document describes generic “networking at sea” capabilities and not a specific network. There are currently a number of tactical operational networks fielded within the allied and coalition communities, the most common being CENTRIXS.

108. A MTWAN is an important step towards a full network centric environment. Figure 1-1 illustrates information exchange domains within the tactical environment. A MTWAN enables full information exchange within the planning and coordination layer and has linkages to the support and real time tactical information exchange layer.

109. A network-enabled approach vice a ‘stovepipe’ platform approach provides a more effective and efficient employment of finite C4 resources and facilitates timely information flow between disparate C4 users.

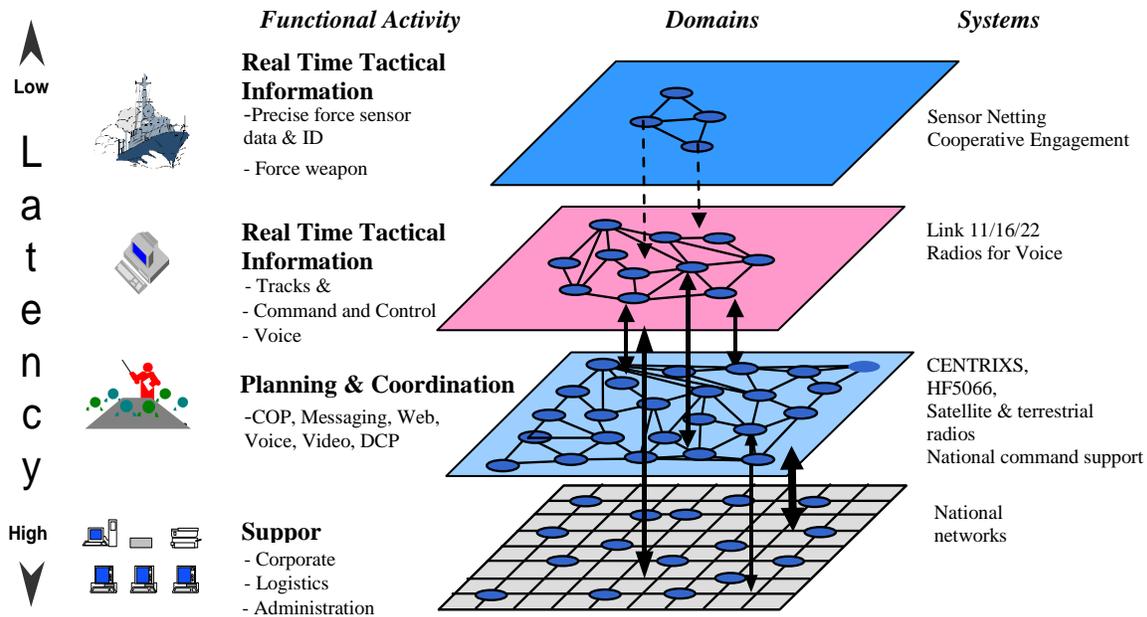


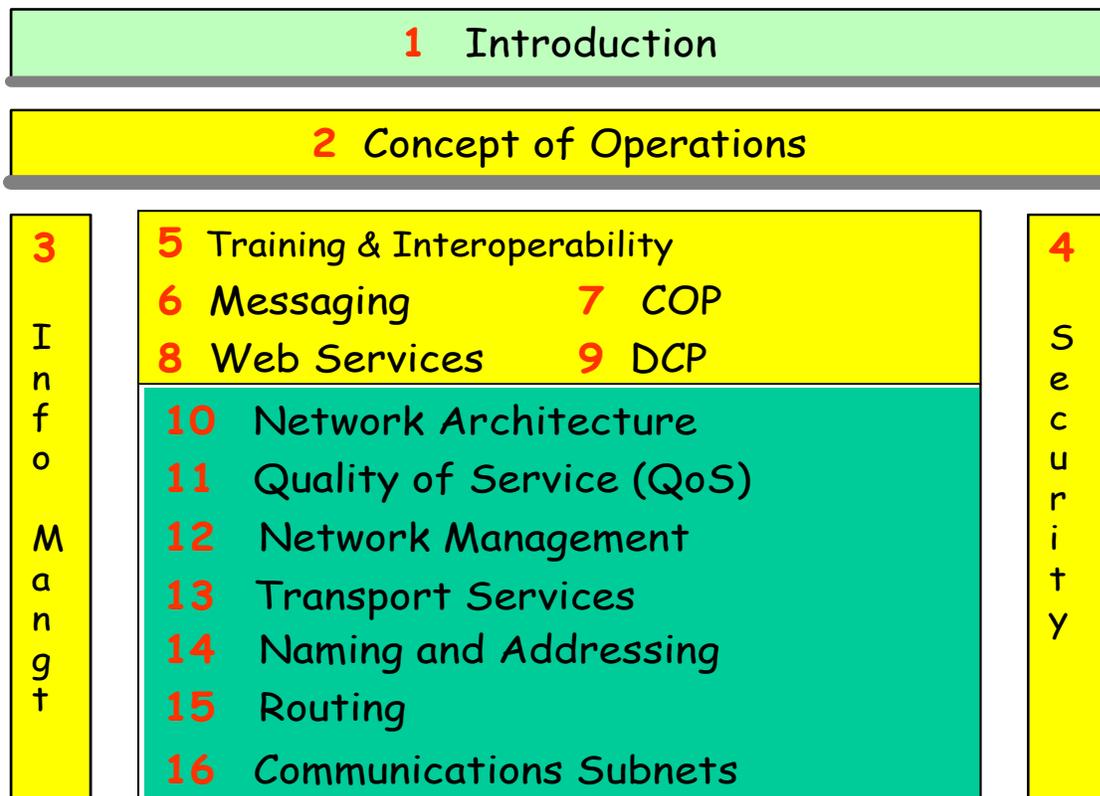
Figure 1-1 Maritime Network Domains

Uncontrolled copy when printed

110. Until nations have implemented the infrastructure required to support the concept of integrated networking, there are likely to be situations where nations will participate under limited conditions. For instance, a unit joining a Multi-National Task Group may only have the capability to support a single HF point-to-point subnet with email capability. In fact, it is likely that a MTWAN would be made up of a combination of stand-alone point-to-point circuits and subnets tied together by nodes using common routing protocols.

DOCUMENT STRUCTURE

111. The document structure is detailed at Figures 1-2 and 1-3. Part 1 (indicated in yellow in Figure 1-2) is focused towards the operators and addresses the information infrastructure (the ‘infostructure’) and associated front-end applications. For the most part, the information in Part 1 is of a general nature that sets the framework for information transfer over a MTWAN and highlights important issues for consideration. Chapters 3 (Information Management) and 5 (Security) are applicable across the breadth of the publication, hence their position within Figure 1-2. Part 2 (indicated in green in Figure 1-2) describes the technical infrastructure. These Chapters provide generic description, while the Annexes are more detailed and include user guides, and technical detail.



Uncontrolled copy when printed

Figure 1-2 Document Architecture

112. The structure of ACP 200 is graphically represented at Figure 1-3. National / Organizational / Enclave variants will be documented in supplements or separate standalone handbooks. Such supplements may or may not refer back to this publication (e.g. ACP 200 NATO-Supp, ACP 200 UK-Supp, CFE CONOPS, CNFC CONOPS, etc). The supplements and handbooks will provide greater detail and information relating to the conduct and operation of national, organization or specific network.

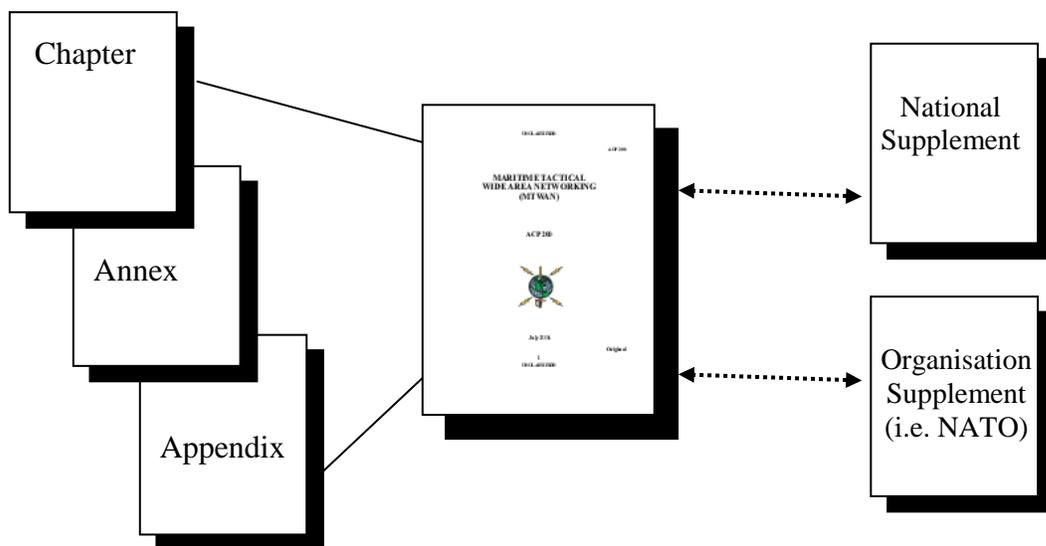


Figure 1-3 Document Structure

CONCLUSION

113. An MTWAN provides an affordable, scalable high-level interoperability solution that can be integrated into existing and future national, combined, joint, allied, and coalition networks to support the tactical user. An MTWAN is an information environment that enhances a Commander's ability to fight and win at sea.

CHAPTER 2

CONCEPT OF OPERATIONS

INTRODUCTION

201. Allied forces have traditionally employed “stovepipe” communications systems to support information exchange requirements. While stovepipe systems can be individually effective, collectively they are equipment intensive, do not enable the efficient use of bandwidth or data throughput, and require the use of military specific equipment and applications.

202. In contrast, IP based networks allow the convergence of many types of data onto a single network. This simplifies the installation, operation and management of equipment and applications, enables the efficient use of communication bearers, and exploits the benefits of IP technology. COTS IP networking products and IP-based information systems support interoperability and provide a large technological base and a cost-effective solution to information exchange requirements.

203. Subsequently, an MTWAN is designed to facilitate information sharing within a maritime force structure, exploiting the benefits of IP technology.

AIM

204. This chapter provides the Concept of Operations (CONOPS) for the establishment and operation of a MTWAN.

SCOPE

205. This chapter uses operational, systems, and technical architectural views to describe the MTWAN CONOPS. A fuller understanding of maritime tactical wide area networking comes from reading the whole publication.

OVERVIEW

206. An MTWAN is based on the following principles:

- a. An IP based network is the most efficient and effective method for transferring planning information within a force;
- b. Information transfer will take place in a Secret-High network;
- c. Connections into/from other networks of a different security domain will be via approved border protection devices; and

- d. Ship-to-ship and ship-shore information transfers will be via a variety of strategic and tactical communication systems.

OPERATIONAL VIEW

207. The MTWAN operational view captures, at a high level, the nature and purpose of information exchanges in an allied tactical environment.

208. Generically, the two types of information used by the tactical user are Action and Planning information. Action information requires immediate action such as attacking the enemy or avoiding attack from the enemy. Action information is therefore extremely time sensitive and is often unique to each individual and platform within the battle space. Planning information is used as a basis for determining future action and is generally not so time sensitive. This information is common to planners and decision-makers throughout the battle space and is normally stored in databases, web pages, or files.

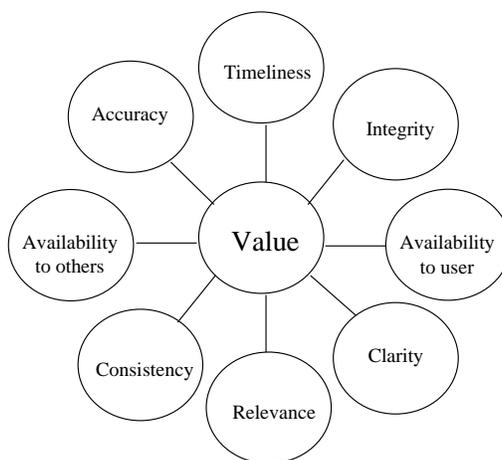


Figure 2–1 Determinants of Information Value

Uncontrolled copy when printed

209. Both types of information are valuable commodities. The extent of their value is determined by the characteristics represented in Figure 2–1. This can be further distilled to describe information in terms of the quality/richness of the information (i.e. the content, accuracy, timeliness and relevance of the information etc), and the degree to which it can be shared (the reach of the information).

210. The OV-1 (Figure 2–2) provides a high-level graphical description of the MTWAN operational concept. It illustrates a maritime Task Force organisation:

- a. Comprising allied / coalition ships, submarines, aircraft, marine, and ground forces as well as associated infrastructure such as Network Operations Centers (NOCs);
- b. Capable of performing the span of maritime operations (i.e. diplomacy, constabulary and military);
- c. With units possibly geographically dispersed; and
- d. With units connected to each other by a variety of RF paths.

211. The end state for any MTWAN improves the richness and reach of planning information across the spectrum of maritime operations through IP networking.

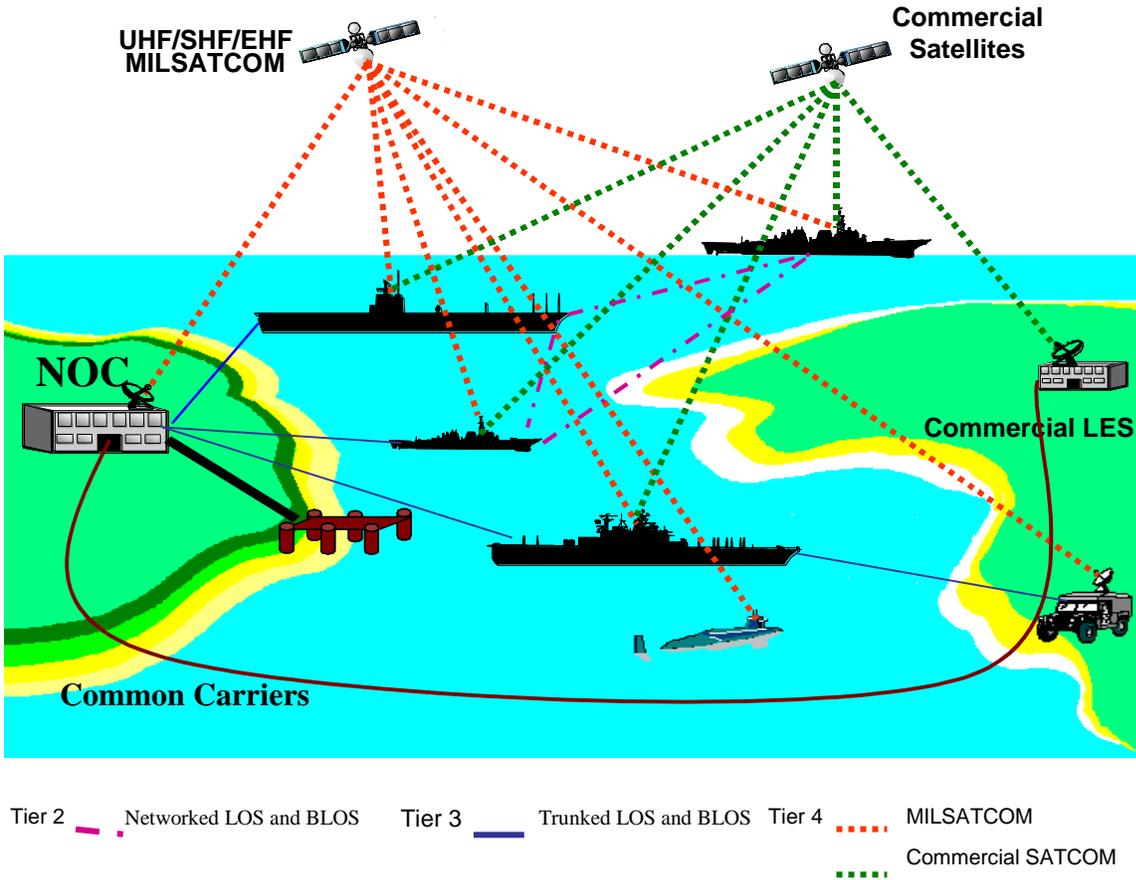


Figure 2–2 Operational View (OV-1)

SYSTEMS VIEW

212. The MTWAN architecture is designed to maximize wide area networking capacity, efficiency, and mobility in a mobile tactical environment. The MTWAN architecture must recognize network limitations and shield them from the users. The infrastructure must be able to change quickly to accommodate intermittent connectivity; varying bandwidth, quality of service and security; and hostile environments.

213. The following systems view provides a description of systems and interconnections to accomplish this in order to support the warfighting functions mentioned in the operational view.

214. The first systems view (Figure 2–3) illustrates a diverse set of communication and information technology infrastructures made interoperable by resources and connectivity protocols (i.e. IP, TCP, UDP, etc). Interoperability is possible because the services and applications above the waist in Foster’s hourglass model (Figure 2–3), and communication

Uncontrolled copy when printed

subnets and computer infrastructure below the waist are channeled through internationally agreed interfaces and protocols.

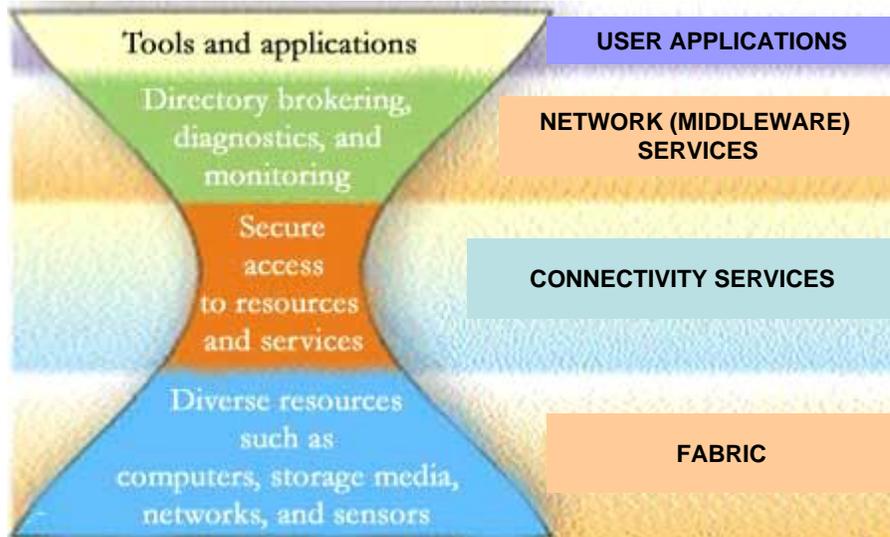


Figure 2-3 Systems View (SV-1.1)

215. IP provides the connectivity needed by user applications and network services, while leaving all other details for definition by whatever lower-level technology is used to realize connectivity services in a particular situation. IP is a very minimal protocol and, essentially, it only has two features—the source and destination end-node addresses carried in the datagram, and the best-effort delivery service.

COMMUNICATIONS ARCHITECTURE

216. The second systems view (Figure 2–4) provides a physical and link view of system components and their interfaces within a MTWAN and also between a MTWAN and external components. In this systems view, the MTWAN is broken up into three segments: shore, space, and deployed.

217. Tier 1 (intra platform and handheld radios): This tier includes shipboard LANs (wired and wireless) and handheld radios. As they are internal to the deployed units they are not actually depicted in the SV-1.2.

218. Tier 2 (wireless networking): Tier 2 is networked LOS and BLOS communications between platforms and expeditionary forces ashore.

219. Tier 3 (wireless trunking): This involves trunked LOS and BLOS communication links, which provide point-to-point connectivity, such as HF BLOS and Digital Wideband Transmission System (DWTS).

220. Tier 4 (satellite communications): This involves military and commercial geosynchronous satellites, such as UFO, SKYNET, GBS/TBS, DSCS, CWSP, IRIDIUM and INMARSAT.

221. A more detailed explanation of the tier system is provided in Chapter 16 (Communication Subnets).

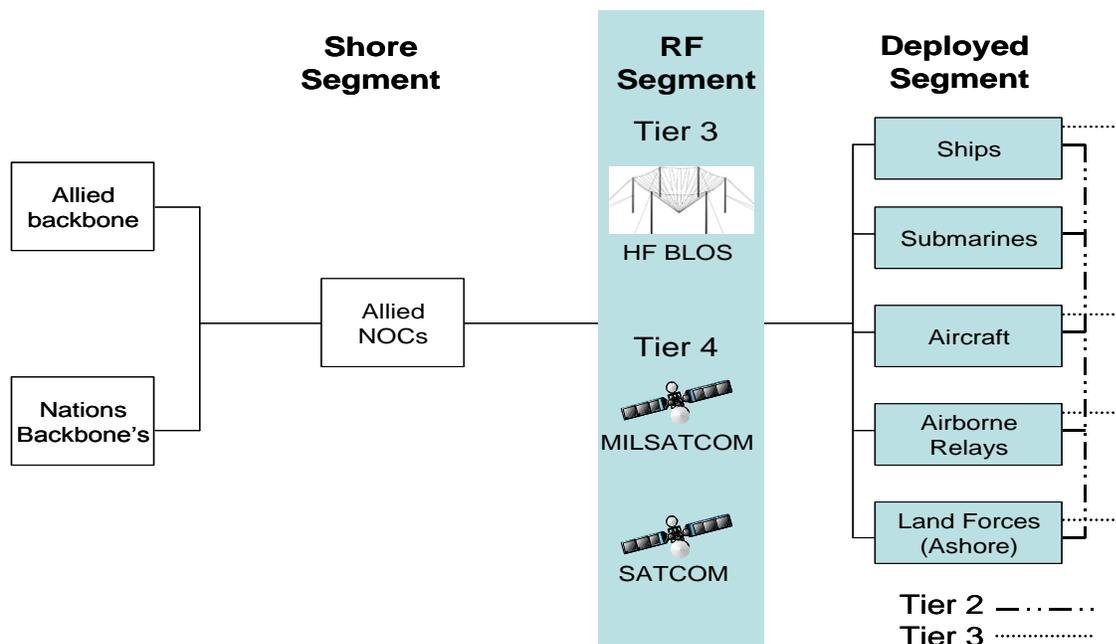


Figure 2-4 Systems View (SV-1.2)

222. Currently, IP connectivity between maritime units (the “as-is” architecture) is achieved by ship-shore point-to-point or point-to-multipoint satellite communications links (i.e. Tiers 3 and 4).

223. However, the key to the success of the maritime communications system is making effective use of all available RF assets (i.e. Tiers 2, 3 and 4). In this regard, the MTWAN seeks to provide a seamless architecture between multiple maritime units networked with differing communications capabilities. An important key to this will be LOS wireless networking (Tier 2) capability such as Sub Net Relay (SNR).

224. This “to-be” architecture emphasizes dense and mesh connectivity. Unlike traditional wireless networks that have a rigid point-to-point or point-to-multipoint structure providing a hub-spoke topology, these networks offer multiple redundant paths and load sharing.

ROUTING ARCHITECTURE

225. In terms of the tier system, the MTWAN should route traffic over the lowest tier whenever possible, in order to mitigate congestion at the higher tiers and make better use of available RF bandwidth.

226. The third system view (Figure 2-5) presents a MTWAN in terms of network topology. SV-1.3 illustrates that a typical MTWAN consists of one or more Autonomous

Systems (AS), each of which in turn comprises a collection of allied units and possibly shore communication stations all connected by a collection of backbone subnets. The MTWAN may be connected to a larger allied network.

227. The implementation of a robust and efficient MTWAN and the provision of a better than 'best-effort' level of service will become essential as data, video and voice are converged onto a single network.

SECURITY ARCHITECTURE

228. The SV-1.3 also represents a secure network established at a Secret-High level. A single security domain at the Secret-High level, as opposed to multiple security domains, enables the timely and efficient exchange of data and reduces network complexity.

229. Approved Boundary Protections Devices (BPD) can be used to allow information to be exchanged between National and Allied domains of different security levels. These may include physical separation (air gaps) policies, approved security guards and firewalls.

230. The 'to-be' multi-level security architecture will be dependent on the development of Multi-Level Security (MLS) products. As BPDs and multi-level security systems become available to nations, policy regarding information flows between national and allied networks should allow for more efficient use of communication resources to meet both allied and national requirements. Until then, nations will have to support separate networks for each security domain.

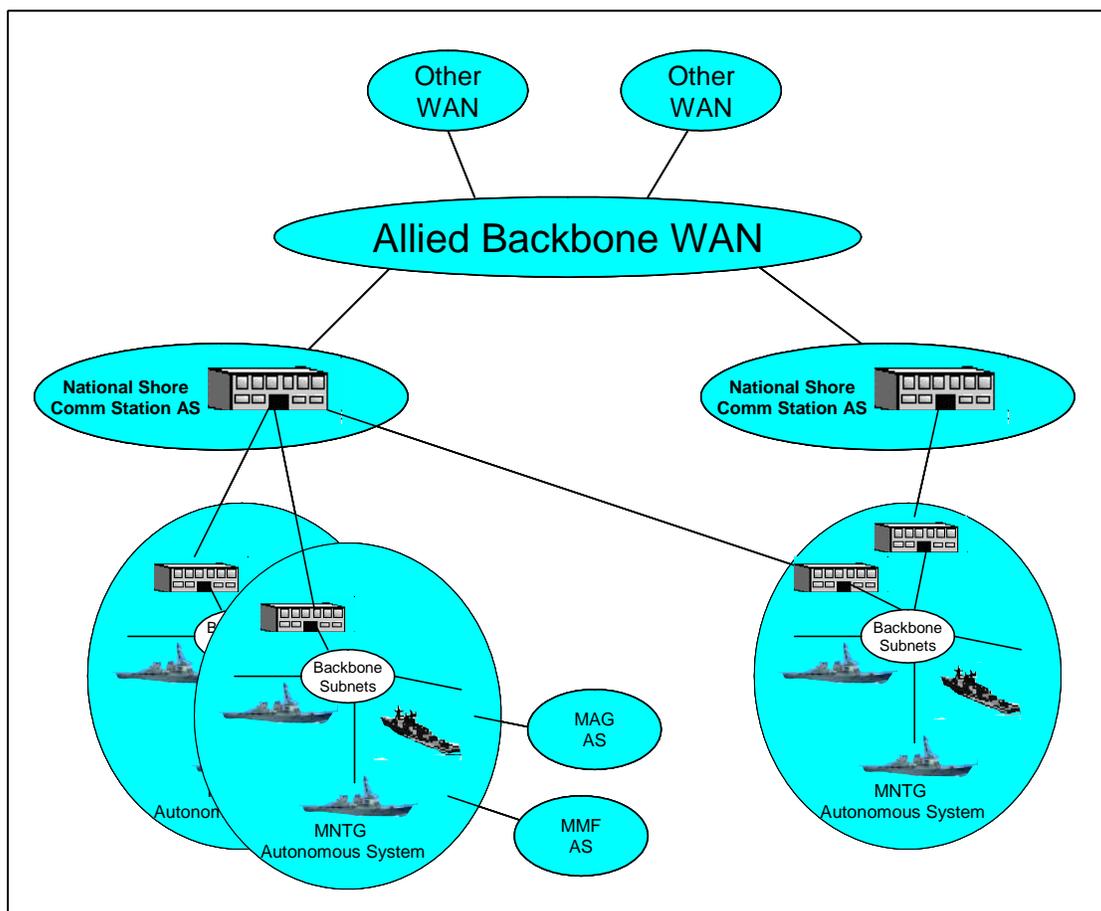


Figure 2-5 Systems View (SV-1.3)

APPLICATIONS / INFORMATION TYPES

231. The network should support the following information types and applications. This is not an exhaustive listing however it describes many of the most prevalent:

- a. High grade (Military) messaging;
- b. E-mail;
- c. Video;
- d. ATO and other large message files;
- e. Imagery including maps and graphics;
- f. Meteorological and Oceanographic data;

- g. Indications and Warning;
- h. Targeting Environment;
- i. Intelligence;
- j. Common Operational Picture;
- k. Collaborative planning tools (such as Chat, Whiteboard, etc);
- l. Web Browsing; and
- m. Voice.

TECHNICAL VIEW

232. The technical view provides the technical foundation for interoperability and the seamless flow of information between maritime forces. Specifically, it provides an example of the rules and standards governing the arrangement, interaction, and interdependence of system parts or elements, whose purpose is to ensure the interoperability among allied units. The technical view is illustrated in Figures 2–6 and 2–7, and is shown to include technical standards, conventions, and rules that govern services and interfaces to support the establishment and operation of a MTWAN.

233. The Communications Subnets, Routing Architecture and Transport Services are the most important layers in a MTWAN technical view. These layers provide a scalable, flexible, interoperable architecture that support a variety of end-user applications and backbone technologies.

234. The implementation of applications and network services in an MTWAN may differ from this publication, and not all backbone technologies listed in TV-1.1 may be employed. Any such differences will be reflected in local network handbooks or supplements to ACP 200. Also, not all end-user applications, network services, and backbone technologies are listed in TV-1.1.

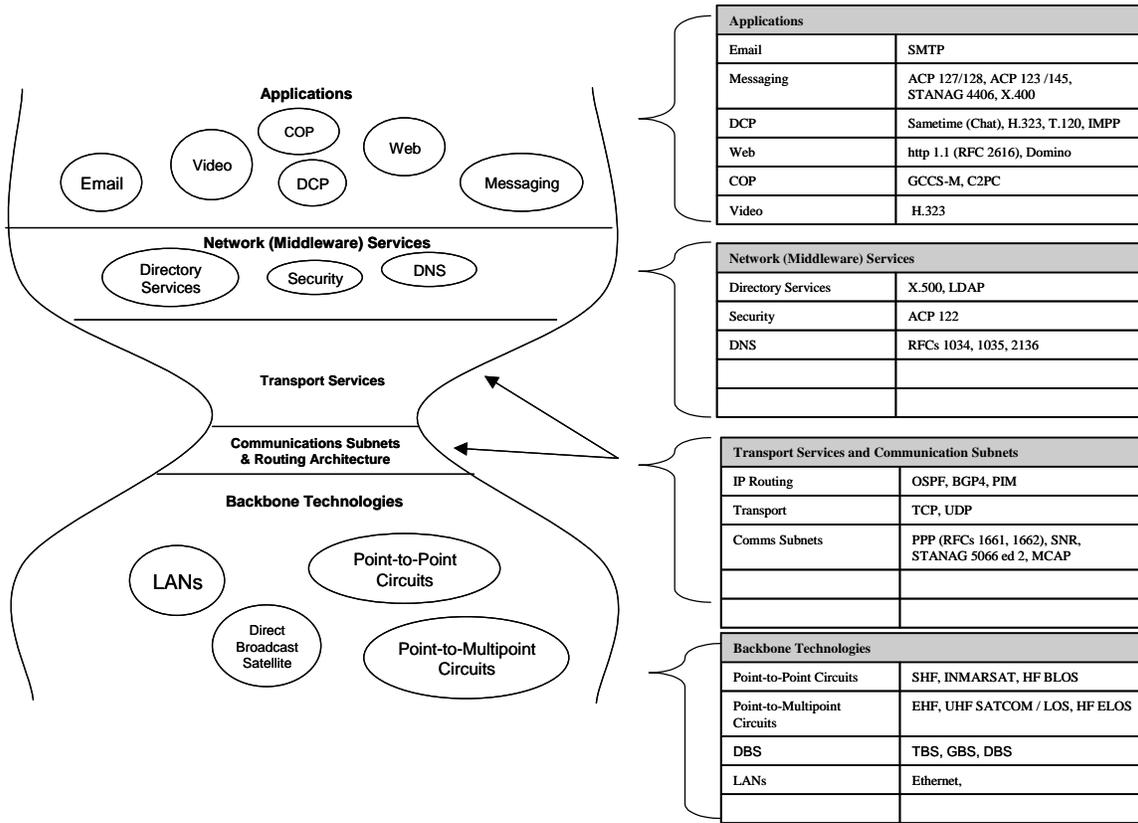


Figure 2-6 Technical View (TV-1.1)

Uncontrolled copy when printed

ROUTING

235. An MTWAN may comprise one or more Autonomous Systems (AS). Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM) will be used for interior routing within an Autonomous Systems (AS) and Border Gateway Protocol (BGP4) for exterior routing between AS. Figure 2-7 depicts a single-AS MTWAN that is divided into a number of OSPF areas. LAN-to-LAN connectivity is provided by the backbone subnets. Details on MTWAN routing can be found in Chapter 15.

COMMUNICATION SUBNETS

236. As shown in Figure 2–7, sending information to a destination on a different LAN, which is itself a subnet, will rely on the forwarding service provided by routers. The routers are connected to each other via MTWAN subnets and each is supported by a communication circuit. Some communication subnets, such as those supported by UHF LOS, HF, and UHF SATCOM require special equipment to interface communication systems to the routers. Details on the communication subnets can be found in Chapter 16.

TRANSPORT SERVICES

237. Most end-user applications use Transmission Control Protocol (TCP) as the transport layer protocol. However, TCP can perform poorly over satellite and multi-member subnets due to long delay and large jitter. As a result, utilization of available bandwidth by applications can be low. Some form of TCP Proxies can be used to improve data throughput for applications over the available communication bandwidth. Multicast (one-to-many) can provide an alternative solution for an efficient use of bandwidth. Studies have shown that many information transfers within a MTWAN are multicast in nature and this can save a significant amount of available bandwidth. Details on Transport Services can be found in Chapter 13.

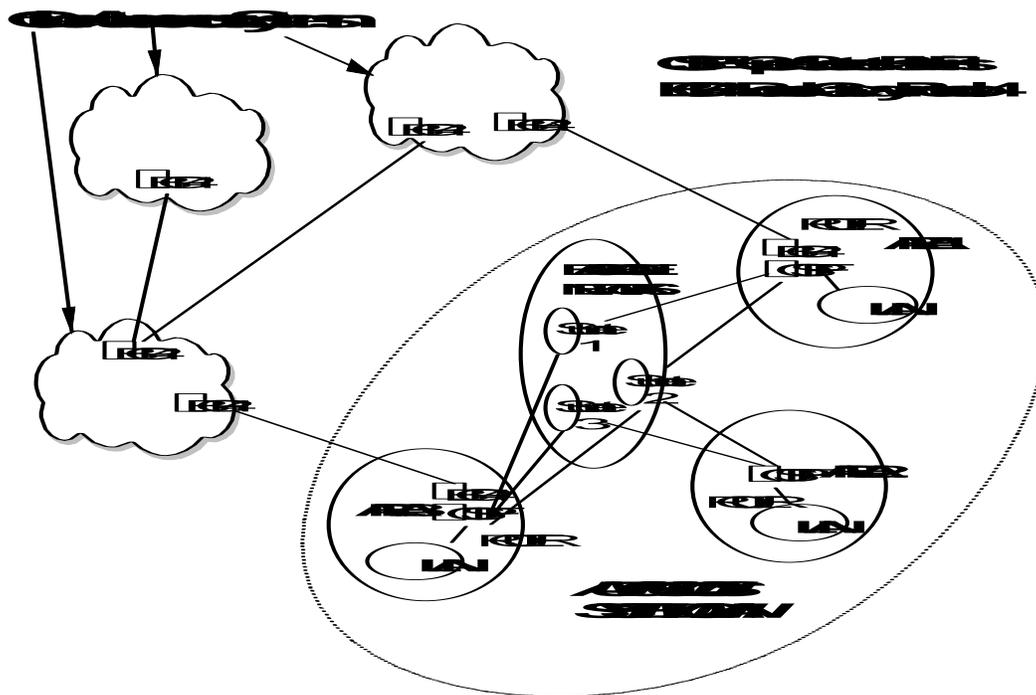


Figure 2-7 Technical View (TV-1.2)

CONCLUSION

238. The MTWAN provides a scalable, flexible, interoperable architecture that support information sharing within a maritime force. The MTWAN improves the richness and reach of planning and coordination information across the span of maritime operations.

Uncontrolled copy when printed

CHAPTER 3

INFORMATION MANAGEMENT (IM)

INTRODUCTION

301. Advances in military communications and Information Systems (IS) provide the modern military commander with information and data faster and more efficiently than at any time in the past. However, these new capabilities are challenging the ability of military commanders to assimilate an ever increasing flow of information, without becoming overloaded.

302. Effective information management provides relevant information to the right person at the right time in a suitable form, to facilitate situational awareness and decision-making. Information is the result of processing data, and managing that information is an integral component of warfare.

AIM

303. This Chapter provides guidance for the efficient collection, collation, storage, processing and display of information to enable faster and more informed decision making in order to successfully complete the mission.

OVERVIEW

304. Data is the representation of facts, concepts, or instructions in a formalized manner suitable for communications, interpretation, or processing by humans or by automatic means. It is only as important as the context within which it is used and the expertise of the individuals using it. Information is the product of the processing of data via the application of procedures, standards, policies, and training. When information is studied within a specific context it leads to knowledge. When knowledge is combined with experience and good judgment, it leads to an informed understanding of the situation, i.e. situational awareness. Enhanced situational awareness subsequently results in an improved decision-making capability. This hierarchy is illustrated in Figure 3-1.

305. High-level guidance for information management will normally be articulated in the Information Management Plan (IMP). The Information Management Plan (IMP) is normally developed by the CCTF Information Management Officer (IMO) and published as an Appendix to the OPLAN. Further information on the IMP can be found in various Multinational Standing documents such as the MNF SOP (v1.6 – February 2006).

306. Naval forces worldwide use Maritime Tactical Messages, standardized general operating instructions known as Operational General (OPGEN) messages, Operational Tasking (OPTASK) messages, and Operational Status (OPSTAT) messages. OPTASK messages provide elements similar to those in the operation plan: situation / mission /

execution / administration / C2 necessary for centralized and decentralized execution in the strategic and operational planning systems. The Officer in Tactical Command (OTC) may detail specific tactical level IM requirements in an OPTASK Information Management (OPTASK IM) message. The format of the OPTASK IM is at Annex A to this chapter.

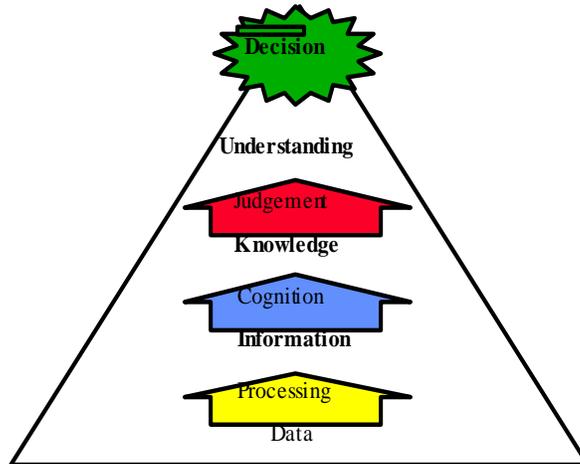


Figure 3-1 IM Hierarchy

DEFINITION

307. IM is a set of integrated management processes and services that enable or allow information producers and consumers to store, locate, retrieve, and transfer the right information, in the right form and of adequate quality, by the most timely, effective, and efficient means in a manner consistent with the Commander's mission.

PRINCIPLES

308. The management of information quality requires a shared concern and pride among information producers and consumers at all levels of Command. The following principles guide best practice in this respect:

- a. Relevance – The information should be of sufficient value that it influences the plan or mission (i.e. the information should address the real needs of the user.);
- b. Accessibility – Information has multiple, even simultaneous uses. Therefore, information should be available to all people that have a legitimate need to know;
- c. Accountability – Individuals are responsible for protecting the confidentiality and integrity of any information they create, utilize, receive, store, or send;
- d. Integrity – Information must be accurate and complete, and requires protection from unauthorised, unanticipated or unintentional modifications;
- e. Clarity – Information should be presented to users in a way that they can understand, properly use, and analyse;
- f. Timeliness - Information is inexhaustible, but its value may perish with time. Rarely is information of value if it is out-of-date or reaches the decision-maker late. Timeliness is typically involved in a trade-off against *accuracy*. The timeliness of information will also influence its *relevance*; and
- g. Consistency – Values and definitions of data must be maintained consistently to ensure that information is understood in the same way when shared e.g. distance should be consistently stated in miles, nautical miles, or kilometers, dependant upon the information domain. To remain consistent users must use it with a common understanding.

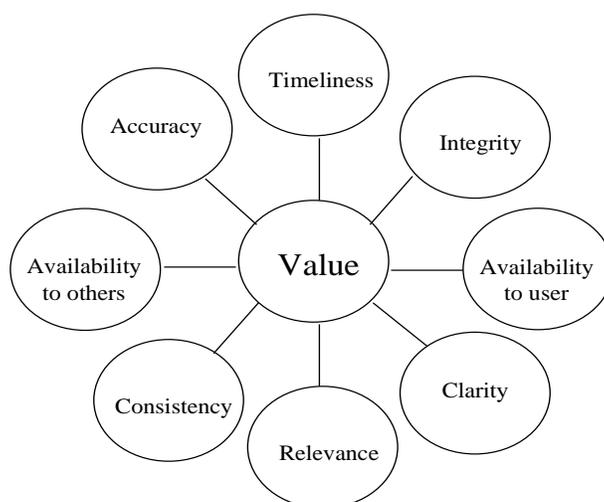


Figure 3-2 Determinants of Information Value

VALUE OF INFORMATION

309. Most of the above principles are also reflected as dimensions that affect the value of information (Figure 3-2) and they are often interrelated. Actions taken to address one dimension of quality may affect other dimensions, often in ways that may not be fully predicted.

310. Users require different degrees of integrity of information, relevance, and accuracy of information. Unfortunately, there is often a trade off between these elements. A highly specific inquiry may require a high degree of accuracy, while a general enquiry may require a high level of relevance. Therefore, in order to maximize effectiveness for any given situation or mission, there may be no single solution.

311. Information must be well organized and presented so that the recipient can use it effectively. Unlike computers, human beings do not simply manipulate numbers according to predefined mathematical rules. They are more adept at recognizing patterns of information and comparing them with past experience or training. Consequently, the manner by which information is presented should focus on displaying those patterns explicitly and without the requirement for the user to waste time and effort in peripheral tasks, such as extracting information from unformatted text. Figure 3-3 is notional, intended solely to emphasize the point that pictures are frequently better than words, and that formatted presentations are typically easier to work with than simple narrative text.

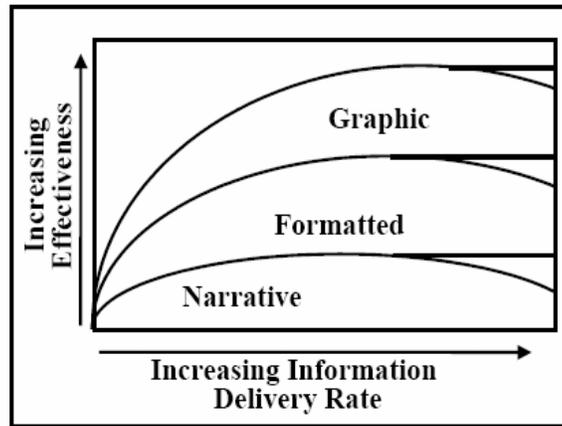


Figure 3-3 Impact of Presentation Form

IM CONSIDERATIONS

312. The application of the key principles governing IM practices and the value of information as outlined above requires some considerations for guiding individual and group behavior. These considerations assist in IM planning and execution:

- a. Information should only be captured once and updated as necessary. Redundant, duplicate, or irrelevant information should be eliminated. Out-of-date data should be archived;
- b. Information should be tailored;
- c. Data definitions must be consistent within a single information domain;
- d. Where information is considered to form part of an official record, additional steps must be taken to ensure all changes are tracked (for example, a document could be backed-up before changes so that copies of all previous versions are available). A version control process should be applied to all official documentation;

- e. Information System managers must ensure that disaster recovery plans exist, are effective, and are periodically tested;
- f. Information must be gathered and maintained in compliance with relevant legal, security and data protection obligations;
- g. Ownership of information will not change throughout its life cycle. Hence, ownership, or the authority under which information is published, must be clear and unambiguous at all times;
- h. Where information is incomplete, it must be highlighted;
- i. The provision of an intermediary between the end-user and the wider community of potential sources of information, so that information is collated and customized according to the user's needs, is encouraged; and
- j. Search engines and smart agents should be used to facilitate the location, acquisition, and retrieval or automatic forwarding of relevant information from multiple sources.

COMMAND AND CONTROL (C2) DECISION CYCLE

313. The C2 decision cycle describes how information contributes to the Command and Control decision-making process. Often described as a series of sequential steps similar to that shown in Figure 3-4, the cycle begins with the collection of information on the current military situation followed by evaluation of this information. A number of Courses of Action (CoA) are then developed from this situational awareness. One or more of these CoAs will be expanded to become a plan (or series of plans) that may then be executed. On completion, the situation is summarized, reassessed, and modified before the cycle begins again. The challenge faced by information managers is the coordination and synchronization of these cycles to compress decision cycles.

314. One essential element of the Information Collection component of C2 Decision Cycle is the Commander's Critical Information Requirements (CCIR). CCIRs are prioritized information requirements that are identified and approved by the commander. Once answered, CCIRs enable the commander to better understand the flow of the operation, identify risks, and make timely decisions to fulfill his intent and retain the initiative.

315. The Commander uses CCIRs to establish the priorities for information gathering, reporting this information, and focusing his staff. They are a tool for the commander to reduce information gaps generated by uncertainties he may have concerning his own force, the threat, or the environment. The aim of CCIRs is to aid the commander by reducing information requirements to a manageable set. Instead of reacting to the threat, commanders are able to maintain tempo by controlling the flow of information necessary to attain an understanding

within the battle space. As events unfold, information requirements may change which in turn requires continual assessment of CCIRs for relevance to current and future situations. Once approved, CCIRs are disseminated by the IMO via the IMP, updated as required, and tracked by the staff. CCIRs may also be promulgated as individual line-items within the OPTASK IM Information Dissemination Plan (IDP).

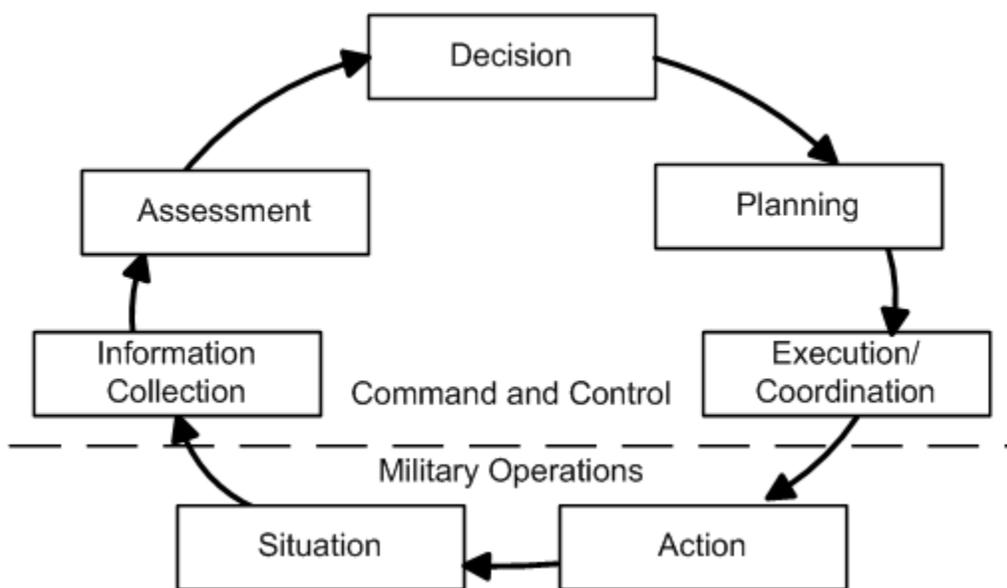


Figure 3-4 C2 Decision Cycle

INFORMATION DISSEMINATION MANAGEMENT (IDM)

316. The IDM is the subset of IM that addresses the end-to-end flow of information — specifically, the compilation, cataloguing, caching, distribution, and retrieval of data (Figure 3-5). Its goal is to provide a managed flow of relevant information based on a commander's mission. This is often referred to as providing the right information, to the right place, at the right time, in the right format.

317. This end-to-end flow of information includes both the flow of information between subordinate and superior commands (i.e. vertically), as well as between peers across the command structure (i.e. horizontally). IDM requires that information is:

- a. **Positioned Properly** – The needs for specific types of information are often predictable. Pre-positioning the required information at the anticipated usage points speeds the flow and reduces overall demands on communication systems and bearers;
- b. **Accessible** – To support concurrent or parallel planning and mission execution, information must be accessible to a wide range of information consumers; and
- c. **Fused** – Users receive information in many formats and from many separate sources, via a range of media. Fusion is the logical blending of this information from multiple and disparate sources into an accurate, concise, and complete picture / summary.

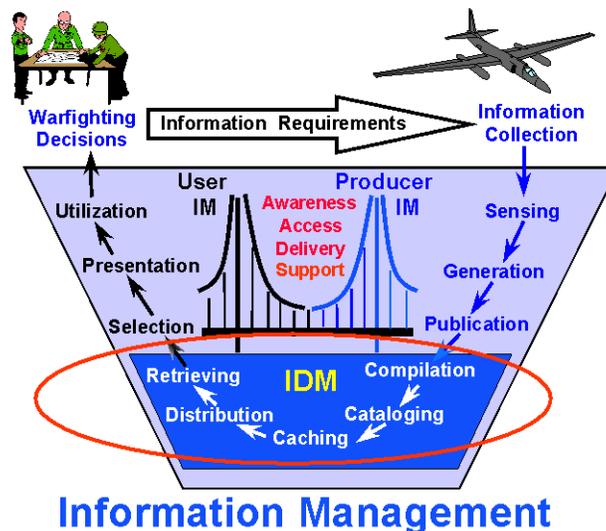


Figure 3-5 IDM

318. Distribution / Retrieval of Information – Information can be positioned properly through push or pull mechanisms:

- a. Push – Information necessary for decision-making is directed (or forced) from the originator to the recipient(s). This may be achieved during radio silence, or EMCON restrictions;
- b. Pull – Information necessary for decision-making is obtained (or requested) by the user. This action requires two-way communications and is not achievable during radio silence (i.e. when a covert EMCON plan is in force);

319. The decision to push or pull may be influenced by:

- a. The relevance of the information;
- b. The information producer's and consumer's situational awareness levels. (I.e. is the information producer aware of the relevance of the information? Is the information consumer aware that the information is available?);
- c. The network infrastructure availability (i.e. a broadcast system may be the only available asset); and
- d. The emission control state of the force (i.e. a COVERT EMCON policy may preclude other means).

INFORMATION DISSEMINATION PLAN (IDP)

320. The Commander's dissemination policy is captured in the IDP and may be promulgated by the OPTASK IM. An IDP describes how the flow of relevant information necessary to support the mission will be managed. It will typically include the promulgation of authoritative data sources, required reports and submissions, unique characteristics of the information architecture, and push / pull guidelines and procedures to be followed. More detailed information as to the contents is provided in the example IDP at Table 3-1.

321. An IDP that is reflective of the daily operations cycle is necessary to ensure information is available when and where required. This cycle is synonymous with "battle rhythm" and is represented in Figure 3-6. The Battle Rhythm reflects the time(s) of day for recurring events and is an essential element in ensuring information is available when and where it is required. How the battle rhythm impacts upon available bandwidth, or vice versa, is depicted in Figure 3-7. All units and supporting agencies should be cognizant of the daily operations cycle.

322. An understanding of peak bandwidth and information usage requirements will assist in the assignment of communications bearers and management of information flow. In the sample daily operations cycle provided in Figure 3-7, ships may have to assign higher data-

rate bearers during the peak times. Low priority traffic (admin and personal) should also be timed for quieter periods.

323. An Information Dissemination Plan (IDP), such as that shown in Table 3-1, helps to regulate the flow of information and assists information producers and consumers in storing and locating information. Additionally, authoritative information sources, information awareness, information access and delivery, and support requirements become more readily apparent to the information consumer.

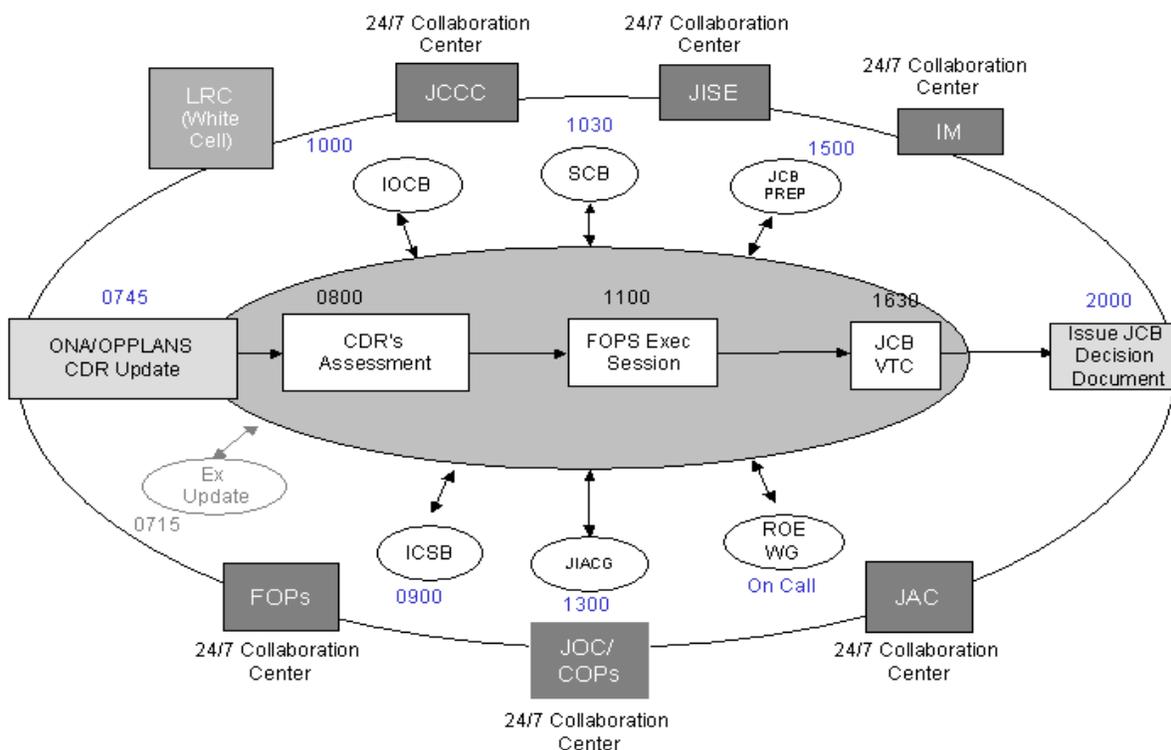


Figure 3.6 Example Battle Rhythm

324. The IDP is a dynamic document and is likely to change throughout an Operation or Exercise.

325. The sample IDP at Table 3-1 highlights the following elements, each of which are considered essential to the Commanders overall IM strategy:

- a. Report Type: Report title or type of information provided;
- b. Submitted By: The unit or agency normally responsible for submitting the report;
- c. As of Time: Close out time for recurring reports, not applicable (N/A) for nonrecurring reports;
- d. Posted NLT: Time to post the report for review;
- e. Where Posted / Transmission Type: The discussion group or web page location to post the report, or the electronic method the information was distributed (i.e. web, e-mail etc);
- f. Notify: Who should be notified after posting a report? Normally not required for recurring reports;
- g. Notification: The preferred method of notifying users following posting;
- h. Precedence: The precedence to use when notifying the report is available (not applicable to some notification methods);
- i. Action Addressees: Lists those that are required to action information that is provided within the document; and
- j. Info To: Lists information addressees.

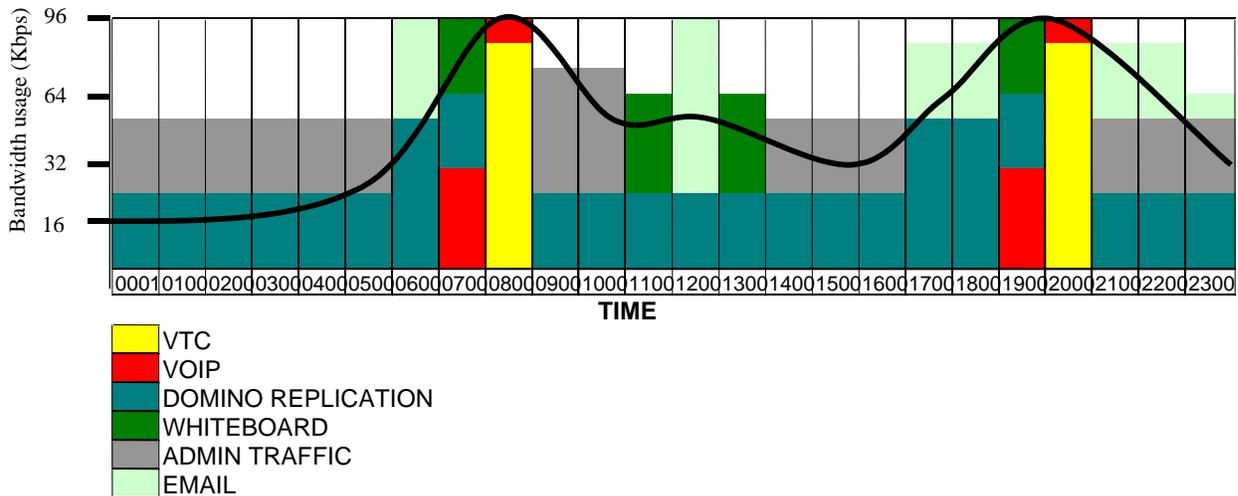


Figure 3-7 Daily Operations Cycle (Notional)

INFORMATION MANAGEMENT TOOLS

326. The rapid development of computing and telecommunications systems has made possible an unprecedented range and variety of information tools. However, in spite of the availability of sophisticated IM tools, it remains the human element that is the most important factor for the effectiveness of information management. Employment of these tools must be consistent, and in accordance with the standards and protocols laid down in Chapters 6 through 9 of this publication.

327. These information tools are themselves both products and determinants of sense making. Information tools affect how people conduct information work, (i.e. searching for information), and how they make sense of the data provided to them.

328. Changing the information tools can change a user's goals (their work or their information tasks), cognition (how they understand their task or the data and its context), behavior (their work, as well as their information seeking and use), and relationships and interactions with their environment. Information systems can alter the relationships between users and tools, and the techniques and systems for data interpretation. In other words, altering the tool can alter the cognitive work. For instance, a decision to promote the use of Web Services (and TTPU: Task, Post, Process, Use) vice email could lead to a greater culture shift in freeing information, thus making it immediately available.

INFORMATION MANAGEMENT IMPEDIMENTS

329. All information users have an inherent responsibility to manage information for their own use and for the use of others. Some impediments and challenges to improving information management include:

- a. Information Overload – Overload occurs when the amount of information received exceeds the ability of users to process it. This can be the result of ambiguous, duplicate, irrelevant, or outdated information. It can also occur when information preparation, such as tailoring and fusion, has failed. Overload can adversely affect IM processes and decrease situational awareness;
- b. Infrastructure – The network must have sufficient capacity, and fail-overs to meet peak demands;
- c. Information Accessibility – Information should be accessible regardless of its location, timeliness, and ownership;
- d. Resources – The previous two points reflect that a significant feature of information management is the balancing of information quality objectives against the constraints of financial and human resources, plus competing demands for more information; and

- e. Lack of an Information Management Culture – An IM culture is required to promote and implement IM best practices. Developing a culture that embraces IM will take much longer than actually deploying the technical infrastructure. Education and understanding at all levels is required before substantial gains in information sharing can truly be enjoyed.

MESSAGE / REPORT IDENTIFIER	SUBMIT BY	SUBMIT AS OF	SUBMIT NLT	TRANSMISSION TYPE	NOTIFY WHO	NOTIFICATION METHOD	NOTIFICATION TIMINGS	ACTION	INFO
OPTASK Unit	All units	1200	1500	E-mail	Not Required	Not Required			As required
Casualty Spot Report	All units	As required	As required	E-mail	Not Required	Not Required			As required
Comm Spot	All units	As required	As required	E-mail	Not Required	Not Required			As required
ROE	Intel	As required	As required	Web site: (Intel folder)	All Units	Chat /Formal Military Message	Immediately	All	CTF
ATO	Air Wing CMDR	1200	1500	Web site: (Strike Ops/ ATO/folder)	All	Chat	Within 30 minutes	All	
OPORDERS	Originator	As required	As required	Web site: (Operations folder)	All	Chat			As required
OPGEN	CTG	As required	As required	Web Site (OPTASK folder)	All	Chat			As required
OPTASK	Warfare Commander	As required	As required	Web Site (OPTASK folder)	All	Chat			As required
NETWORK CONFIGURATION PLAN	CTG	As required	As required	Email/Web Site (Network folder)	All	Chat/Formal Military Message/Email			As required
Wx Observation	MET Guard	1200 2359	1300 0100	Email (Action): Web Site (METOC folder) for info addressee	As Required	Chat	Within 30 minutes		

Uncontrolled copy when printed

Table 3-1 Example Information Dissemination Plan (IDP)

MINIMIZE

330. The transmission of routine administrative traffic must be minimized in order that information essential to the current operation can be transferred. Although the term “minimize” is typically employed in messaging systems, it can be used effectively across all information systems. Full details of the Minimize Procedure are contained in ACP 121.

OPSEC – RIVERCITY PROCEDURES

331. RiverCity procedures are used to control outgoing communication paths for OPSEC reasons. The direct access to an open channel of communication ashore has a number of operational implications. This, combined with direct access to e-mail, carries an inherent risk of essential elements of friendly information being disclosed, either deliberately or inadvertently. IT security measures, including what information can / cannot be passed, must be well understood by all. Accordingly, RiverCity procedures must include a plan to shutdown / limit access to personal e-mail services and Internet access when required for reasons of operational security, or in the event of a significant incident at sea.

FILE NAMING CONVENTION

332. Users should focus on providing a meaningful description for all file names. The following document-naming convention allows other users to locate, read, and ascertain exactly WHAT it is, WHEN it was created, WHO created it, and its CLASSIFICATION.

333. The following naming convention shall be used:

- a. Name – provide a meaningful name (e.g. INTSUM);
- b. Date – This date may be the date that the document was signed, or the brief was presented, or the authoring date. The date format must be DDMMYY;
- c. Author – who created the document (e.g. J2); and
- d. Classification – as assigned by the originator. For example:
 - (1) U = Unclassified;
 - (2) R = Restricted;
 - (3) C = Confidential;
 - (4) S = Secret; and
 - (5) TS = Top Secret.

334. The Releasability caveat as detailed in the OPTASK IM must be included if necessary.

335. The following is an example of what the file name of an INTSUM document created on 21 May 05, by the CJTF 950 Intel Department, and with a CONFIDENTIAL classification would look like:

INTSUM_21MAY05_J2_C

CONCLUSION

336. While information has always been a source of power, it is now increasingly a source of confusion. Understanding and implementing the concepts of this chapter will reduce confusion, and allow the ready assimilation and use of information by the warfighter to enhance decision-making.

OPTASK IM – INSTRUCTIONS

1. The purpose of the OPTASK IM is to list dynamic IM issues pertinent to IP networking in the maritime tactical environment. The format of the OPTASK IM is based on the Message Text Format (MTF), which consists of a number of sets with each set composed of a number of fields. The OPTASK IM message consists of the following sets, where C indicates Conditional sets, O indicates Optional sets, M indicates Mandatory sets, and R indicates Repeatable sets:

Note: This message format is published here pending inclusion in APP-11. The current edition of APP-11 should be consulted to ensure there is not a more up-to-date version of this message format.

LINE	USAGE	SET NAME	SET TITLE	FIELD DESCRIPTION
1	C	EXER	Exercise Identification	Provides the designated code name which supports an exercise
2	O	OPER	Operation Identification	Provides the designated code name which supports an operation
3	M	MSGID	Message Identification	Provides a description of the message. The MSGID fields are: MTF Name (M) i.e. OPTASK IM; Originator (M); Message Serial Number (O); and Month (O)
4	O / R	REF	Reference	Provides both MTF and non-MTF references. The REF fields are Serial letter (M); Communications type (M) e.g. DOC, MSG; Originator (M); DTG of reference (M) e.g. 26APR2006; Message or document serial number (O); Special notations (O) e.g. NOTAL; and Subject Indicator Code (O)
5	M	PERIOD	Period of Time	Provides the effective time period of the OPTASK IM message (generally the same as the OPGEN). The PERIOD fields are Start time (M); and Termination time (M)

LINE	USAGE	SET NAME	SET TITLE	FIELD DESCRIPTION
6	O / R	POC	Point of Contact	Provides a point of contact information for the message. The POC field are: Contact name (M); Rank or position (M); Unit Identifier (M); Location (M); and Contact type (M) e.g. TEL SECTEL
7	M	GENTEXT/ PURPOSE	General Text/ Purpose	Provides the purpose of this OPTASK IM, and should relate to the guidance provided in the OPGEN.
8	M	GENTEXT/ IER POLICY	General Text/ Information Exchange Requirement Policy	Allows Commanders to emphasize specific requirements of information to be exchanged throughout the network. It can be used to explain the intent behind the policies listed in this segment.
9	O	OBJECTIVES	General Text/ Objectives	Lists the objectives of this OPTASK IM.
10	M / R	IDP	Information Dissemination Policy	Describes how the flow of relevant information necessary to support the mission will be managed. The IDP fields are: Message or Report Identifier (M); Submit by (M); Submit as of (M); Submit no later than (O); Transmission type (M); Notify who (O); Notification Method (C); Notification Timing (C); Action (To) Addressees (C); and Information (cc) Addressees (O)
11	M	CPOS	Commanders Priority of Service	Establishes the Commander's priorities for applications and services. It may also be used to inform quality of service settings within the OPTASK NET. Table 3-B-1 provides the key for use in this set. This can be added to by the inclusion an amplification remark located within brackets immediately after the letter identifier. In the following example the Commander has stipulated that the priority of service is to be chat, followed by secure email with attachments then web services and COP. Example: POS/I/B/F/G//

LINE USAGE SET NAME SET TITLE FIELD DESCRIPTION

ID	Application/Service	ID	Application/Service
A	Classified Email	J	White-boarding
B	Classified Email with attachments	K	Screen Sharing
C	Classified Email with attachments/PKI	L	Application Sharing
D	Unclassified Email	M	Voice
E	Personal Email	N	VoIP
F	Web Services	O	VTC
G	COP	P	Web Video
H	Internet Browsing	Q	POTS
I	Chat	R	Replication

Table 3-A-1 – Priority of Service (POS) Key

12	O	GENTEXT/ EIE POLICY	General Text/ Electronic Information Exchange Policy	Allows Commanders to emphasize specific aspects of the Electronic Information Exchange Policy. It can be used to explain the intent behind the chat, email and other policies listed below.
13	M	GENTEXT/ FILE SIZE	General Text/File Size	Stipulates the maximum permissible file size for email and chat attachments and if necessary for web pages/links. It is unlikely that there will be a uniform policy across a TF due to the different IER for platforms, e.g. Force level ships can be expected to have greater IER requirements and communications capabilities than unit level ships.
14	O	GENTEXT/ ATTACHPOL	General Text / Attachment Policy	Allows the Commander to specify any requirements for attachments, such as the file extensions permitted. All attachments are to be scanned for viruses prior to transmission. It is possible that different guard rule sets will be enforced within national gateways and possibly between enclaves. In such cases the OPTASK IM should clearly lists the attachment policy for each domain if relevant.

LINE	USAGE	SET NAME	SET TITLE	FIELD DESCRIPTION
15	O	GENTEXT/ COMPRESSPOL	General Text / Compression Policy	Allows the Commander to stipulate any file compression policy to be adopted, for example the Commander may require that files over 1.4 be zipped using an approved ZIP program. File compression results in a reduction in required storage space and bandwidth for transmission. Network specific compression measures will be detailed in the OPTASK NET.
16	M / R	CAVEAT	Caveat	Lists any unique labeling and/or caveats. Messages not bearing the necessary classification and caveats may not be permitted to pass through the Secure Gateway or Mail Guards that may be in use on the network.
17	M	GENTEXT/ OPSEC	General Text / Operations Security	Allows the Commander to stipulate specific OPSEC requirements. This may include River City procedures, which may be articulated within the OPTASK IM or referenced in another publication.
18	M	GENTEXT/ MINIMIZE	General Text / Minimize	Stipulates the processes to be followed when Minimize procedure is implemented on IP networks.
19	O	GENTEXT/ WEB SERVICES	General Text/ Web Services	Allows the Commander to emphasize key aspects of its web services strategy. It can be employed to distinguish each separate web service provided on the network. Web Services promotes authoritative data and its reuse and allows information consumers the capability to access the data they need, when they need it, from wherever they are.
20	M	GENTEXT/ REPPOL	General Text / Replication Policy	Allows the Commander to stipulate the TF / TG replication policy, including how often web sites should replicate and an indication of likely replication times across the TF / TG

LINE	USAGE	SET NAME	SET TITLE	FIELD DESCRIPTION
				<p>Details the authority for which each media type can be used by drawing from the Table 3-B-2.</p> <p>Example: ACE1/CE23/ACEF4/B5/AF6/FG7 indicates that the Commander has approved:</p> <ol style="list-style-type: none"> 1) Email, Web replication, and ACP127 / 128 messaging may be used to pass Administrative and Non-Mission Essential Traffic. 2) Web replication and ACP127 / 128 messaging may be used to pass executive orders, directives, and regularly promulgated updates and summaries. 3) Email, Web replication, ACP127 / 128 messaging and chat may be used to pass non-regularly promulgated updates and summaries. 4) Email with PKI to be used to pass ROE. 5) Email and chat may be used to pass TACSIGs. 6) Chat may be used for Immediate Action Orders and Coordination.
21	M / R	MESSAGE	Message	

Transmission	
A	Email
B	Email with authentication
C	Web Replication
D	Web Replication with authentication
E	ACP 127/128
F	CHAT
G	Voice

Content	
1	Administrative and Non Mission Essential Traffic e.g. PERSTAT, OPDEF, etc.
2	Executive Orders and Directives, e.g. OPGENs, OPTASKs, etc.
3	Regularly promulgated updates and summaries e.g., ATO, OPSUM Feeders, OPSTATs etc.
4	Non-regularly promulgated updates and summaries e.g., CCIR, RFI etc.
5	Rules of Engagement.
6	TACSIGs IAW ATP1 Vol I article 4124.
7	Immediate Action Orders and Coordination e.g. NGS, track deconfliction, weapon engagements.

Table 3-A-2 – Message Field Set

Uncontrolled copy when printed

LINE	USAGE	SET NAME	SET TITLE	FIELD DESCRIPTION
22	M	GENTEXT / CHAT POLICY	General Text/ Chat Policy	Allows the Commander to promulgate any specific requirements relating to the use of text-based chat.
23	M / R	CHAT	Chat	Provides the Scheduled Meeting Rooms and the associated monitoring requirements for each. The Chat fields are: Name (M), Purpose (M), Members (M), Moderator (M), Guard Requirements (M)
24	O	GENTEXT / VTC	General Text/ Video Tele Conference	Allows the Commander to detail specific VTC requirements, policies and procedures.
25	O	GENTEXT / VOIP	General Text/ Voice of Internet Protocol	Allows the Commander to detail specific VOIP requirements, policies and procedures.
26	M	GENTEXT / POWERPOINT	General Text/ PowerPoint	Allows the Commander to list the standard PowerPoint policies that are to be used when creating presentations in PowerPoint (see Annex C).
27	M	GENTEXT/ SOFTWARE	General Text/ Software	Detail specific policies and procedures for downloading and installation of software.
28	O	GENTEXT/ STORPOL	General Text/ Storage Policy	Allows the Commander to emphasize specific aspects of the Storage Policy
29	M	GENTEXT/ ARCHPOL	General Text/ Archive Policy	Allows the Commander to stipulate the length of time that records are to be retained. This does not override National Archival responsibilities.
30	M	FNP	File Naming Policy	Allows the Commander to stipulate the file naming structure to be used for the period of the operation/exercise, or reference ACP200 Chapter 3.
31	O	AKNLDG	Acknowledge	Provides operator acknowledgement and not communications center acknowledgement instructions.
32	M	DECL	Declassification	Provides declassification or downgrading instructions, if the message is classified.

OPTASK IM (EXAMPLE)

EXER/EXAMPLE 06//

MSGID/OPTASK IM/CTG xxx.x/000/MAR//

REF/A/DOC/MPAT/6FEB2006/-/MNF SOP V1.6//
REF/B/DOC/CCTF/OPLAN ANNEX x APPENDIX A//
REF/C/DOC/CCEB/MAY2005/-/ACP200(B)//
REF/D/MSG/CFMCC/281210ZDEC2006/002/OPGEN//
REF/E/GENADMIN/CFMCC/130145ZDEC2006/003/OPTASK COMMS//

NARR/REF A IS MNF SOP V1.6, REF B IS CCTF IM GUIDANCE FOR EXER EXAMPLE 06, REF C IS ACP 200 (A) - MARITIME TACTICAL WIDE AREA NETWORKING, REF D IS CFMCC OPGEN, REF E IS CFMCC OPTASK COMMS//

PERIOD/160001ZMAY2006/262359ZMAY2006//

POC/SAMPLE.R/CDR/CTG xxx.x IMO/LOC: USS SAMPLE/POTS:(701) 123-1234/EMAIL: SAMPLE.R(AT)NAVY.MIL//

GENTEXT/PURPOSE/TO DEFINE INFORMATION OF A DYNAMIC NATURE REQUIRED TO PROVIDE INFORMATION SHARING AND KNOWLEDGE MANAGEMENT ACROSS IP NETWORKS IN THE MARITIME TACTICAL ENVIRONMENT//

GENTEXT/IER POLICY/IMPROVING THE MANAGEMENT OF INFORMATION IS A RESPONSIBILITY THAT IS SHARED BY ALL INFORMATION PRODUCERS AND USERS. THE IMPROVEMENT IN THE QUALITY OF INFORMATION THROUGH IM CAN RESULT IN BETTER AND FASTER DECISIONS//

GENTEXT/OBJECTIVES/1. USERS GET ALL THE INFORMATION NEEDED IN THE DESIRED CONTEXT/2. PROMOTE AUTHORITATIVE DATA AND ITS REUSE/3. ALLOW USERS TO COLLABORATE EFFECTIVELY REGARDLESS OF GEOGRAPHIC LOCATION//

IDP/ATO/AIR WING CDR/ASOF1200/NLT:1400/POST – STRIKE OPS-ATO FOLDER//
IDP/COMMSPOT/ALL UNITS/AS REQD/-/EMAIL/CTG/CHAT//
IDP/OPGEN/CTG/AS REQD/-/POST – OPGEN FOLDER//
IDP/OPORDERS/ORIGINATOR/AS REQD/AS REQD/POST – OPS FOLDERS//
IDP/OPREP FEEDER/ALL UNITS/ASOF:2359/NLT:0200/EMAIL/CTG/CHAT//
IDP/OPSTAT UNIT/ALL UNITS/ASOF:1200/-/EMAIL/CTG/AS REQD//
IDP/ROE/INTEL/AS REQD/POST – ROE FOLDER/ALL UNITS/CHAT//
IDP/WX REPORTS/MET GUARD/ASOF:1200 AND 2359/POST – METOC FOLDER/ALL UNITS/CHAT//
CPOS/CTG/I/B/F/G/N/K/H//

GENTEXT/EIE POLICY/THE EASE OF EMPLOYMENT OF ELECTRONIC EXCHANGE TOOLS SUCH AS EMAIL AND CHAT SHOULD NOT RESULT IN INFORMALITY OR LAX PRACTICES. BEST PRACTICES PROVIDED IN THE EMAIL AND CHAT USER GUIDES WITHIN REF C SHOULD BE FOLLOWED//

GENTEXT/FILE SIZE/ FORCE LEVEL PLATFORMS HAVE UNRESTRAINED USE BUT SHOULD EXERCISE BEST PRACTICES. INFORMATION PRODUCERS ARE TO REDUCE FILE SIZES WHERE POSSIBLE. NO UNNECESSARY GRAPHICS ARE TO BE INCLUDED//

GENTEXT/ATTACHMENT POLICY/EMAIL AND CHAT ATTACHMENTS SHOULD NOT EXCEED 1.4 MB. ALL ATTACHMENTS ARE TO BE SCANNED FOR VIRUSES PRIOR TO TRANSMISSION. ATTACHMENTS ARE TO BE LIMITED TO TEXT (.TXT), MS OFFICE FILES (.DOC .XLS .PPT), GRAPHICS (.JPG, .BMP, .GIF), ADOBE (.PDF), AND WEB (.HTM, .XML)//

GENTEXT/COMPRESSION POLICY/FILES LARGER THAN 1.4 MB ARE TO BE ZIPPED. NETWORK COMPRESSION MEASURES ARE DETAILED IN THE OPTASK NET//

CAVEAT/UNCLASSIFIED REL GCTF-CNFC//
CAVEAT/CONFIDENTIAL REL GCTF-CNFC//
CAVEAT/SECRET REL GCTF-CNFC//

GENTEXT/OPSEC/CONTENT PROVIDERS ARE TO ENSURE DISCLOSURE PRINCIPLES ARE FOLLOWED CLOSELY. RIVER CITY PROCEDURES IAW REF xx ARE IN FORCE//

GENTEXT/MINIMIZE PROCEDURES/MINIMIZE PROCEDURES ARE IAW ACP121. IF IMPOSED, EMAIL AND CHAT ATTACHMENTS ARE TO BE LIMITED TO 50 KB UNLESS MINIMIZE CONSIDERED IS AUTHORISED. QUOTE MINIMIZE CONSIDERED UNQUOTE IS TO BE INCLUDED IN THE EMAIL SUBJECT HEADING//

GENTEXT/WEB SERVICES/CFMCC INFORMATION IS FOUND AT THE CCTF WEBSITE VIA THE CFMCC TAB AT [HTTP://xxx.xx.xx.xx/EXERCISE/SAMPLE/SITE.NSF](http://xxx.xx.xx.xx/EXERCISE/SAMPLE/SITE.NSF). THE PLANNING WEBSITE IS AT [HTTP://xxx.xx.xx.xx/EXERCISE/PLANNING/SITE.NSF](http://xxx.xx.xx.xx/EXERCISE/PLANNING/SITE.NSF). WEB EDITORS ARE TO ENSURE WEBPAGES ARE ACCURATE AND CURRENT AT ALL TIMES. CONTENT MANAGERS SHALL ENSURE POSTED INFORMATION IS RELEVANT AND IAW WITH THE IDP. UNITS ARE TO PASS EMAILS WITH LINKS VICE ATTACHMENTS. PPT SHOULD BE OPTIMISED USING APPROVED TOOLS WHERE AVAILABLE//

GENTEXT/REPLICATION POLICY/CAS DOMINO SERVER REPLICATION HALF HOURLY, CHAT DB EVERY TWO MINUTES//
MESSAGE/ACE1/CE23/ACEF4/B5/AF6/FG7//

GENTEXT/CHAT POLICY/ CHAT PROCEDURES DETAILED IN REF x ARE TO BE USED. CHAT WILL BE EMPLOYED TO SUPPORT TACTICAL AND OPERATIONAL OBJECTIVES AND MAY BE UTILISED IN ALL WARFIGHTING ENVIRONMENTS. CHAT WILL ONLY BE USED FOR THE PROFESSIONAL EXCHANGE OF INFORMATION. PARTICIPANTS MAY MONITOR CHAT ROOMS FOR SITUATIONAL AWARENESS (SA), HOWEVER ARE NOT PERMITTED TO TRANSMIT UNLESS IN PURSUIT OF DUTIES. CHAT ROOM MODERATORS

DUTIES ARE DETAILED AT REF x, MODERATORS MAY ALSO LIMIT CHAT ROOM PARTICIPANTS. WHISPERS ARE TO BE KEPT TO A MINIMUM//

CHAT/CMD/CDR TACTICAL AND ADMIN ORDERS/ALL UNITS BWC, PWO, TAO, ORO/CTG xxx.x/GUARD//

CHAT/INTEL/COORDINATE AND DEVELOP INTEL EFFORTS/ALL UNITS/CTG xxx.x/WHENDI//

CHAT/COMM/ENGINEER C4I AND HELPDESK ISSUES/ALL UNITS/JCCC/WHENDI//

CHAT/MIO/MONITOR INTERDICTION ACTIVITY/ALL TG xxx.x UNITS/CTG xxx.x/GUARD//

CHAT/COPS/COORDINATE TACTICAL AND ADMIN OPS FROM PRESENT TO 24 HOURS OUT/ ALL UNITS BWC, PWO, TAO, ORO/CFMCC BWC/GUARD//

GENTEXT/VTC/CCTF AND CFMCC BATTLE RHYTHM WILL DICTATE THE VTC SCHEDULE. VTC IS TO BE USED AT COMMANDERS DISCRETION AND IAW IDP//

GENTEXT/VOIP/IAW IDP. VOIP WILL PROVIDE SECURE VOICE CONNECTIVITY UP TO AND INCLUDING SECRET REL xxxxx//

GENTEXT/POWERPOINT/POWERPOINT PRESENTATIONS SHALL CONFORM TO BEST PRACTICES AS CONTAINED IN REF C//

GENTEXT/SOFTWARE/SOFTWARE IS NOT TO BE DOWNLOADED NOR INSTALLED BY UNAUTHORISED PERSONNEL. UNITS ARE TO ENSURE THAT NECESSARY SOFTWARE INSTALLED IAW THE OPTASK NET//

GENTEXT/ARCHIVAL POLICY/RECORDS ARE TO BE RETAINED UNTIL THREE MONTHS AFTER THE COMPLETION OF THE OPERATION TO ALLOW FOR COMPILATION OF LESSONS LEARNT. THIS DOES NOT OVERRIDE NATIONAL ARCHIVE POLICIES AND RESPONSIBILITIES//

FNP/IAW ACP200 - ANNEX A TO CHAPTER 3//

AKNLDG/ALL ACK//

DECL/-/-/DATE:26062006/X1//

FILE COMPRESSION

INTRODUCTION

1. File compression technologies compact electronic files in order to minimize the size of created files. This results in a reduction in required storage space and bandwidth for transmission.

AIM

2. This Appendix provides a framework for file compression across low bandwidth tactical networks.

OVERVIEW

3. File compression reduces the overall space taken up by a file or set of files for transfer, downloading and backup. Reducing file size has become paramount not only to avoid network traffic congestion but to also minimize the users download time as users increasingly rely on formatted presentation / information (vice simple narrative text) and use of web services.

4. A number of different compression methods have become standardized across computing technologies and are widely used (ZIP, GIF, and JPEG). Automated compression technology, which does not require any user intervention, should be utilized when available.

5. The file compression technique for any operation / exercise will be determined by the Commander and promulgated in the OPTASK IM Line 15 (COMPRESSPOL).

6. Knowing which compression technique to use in order to maximize efficiency is difficult and to an extent self-defeating if the goal is to encourage widespread use. Warfighters do not have the available time to select the proper compression method from a huge list of options. A general understanding of the common compression technologies, in addition to providing a simple and limited compression framework, should provide a higher adoption rate. Automated compression technology should be utilized when available to provide a “safety net” for users who fail to use file compression.

COMPRESSION

7. File compression is performed by a software program that uses an algorithm to compress or decompress data. In the context of electronic files, compression can be categorized into three areas:

- a. Static — typically archived and not usable in its compressed state. Must decompress file before useful. Example: ZIPed file.

Warning: When using static compression, the end-user of the information must have the appropriate (same) de-compression tool available.

- a. Processed — similar to static compression, but file is usable in its compressed state. Example: JPEG image. Imagery, audio, and video files can be saved in “lossy” or lossless formats; and
- b. Dynamic — also known as streaming, where content is compressed on delivery and uncompressed on arrival to your computer. Example: networked video stream.

8. There are several other more specialized compression categories (including database compacting and computer backup utilities) but these categories are proprietary.

FILE SIZE

9. There is a direct correlation between the size of a file and the fidelity of information within the file. Text, whether a letter of alphabet, a number, or special character typically represents the smallest file sizes. In contrast, an image’s file size is determined in pixels and colour dimensions. Subsequently its file size is a factor of the Dots Per Inch (DPI), the image size in pixels, and the colour depth.

SELECTION

TEXT

10. There are a number commercial file compression programs available which provide approximately the same compression ability. User functionality and features usually define the differences, thus leading to user preference as the deciding factor. The key is to designate a network standard in order to ensure all parties have the ability to both compress, and decompress the data.

IMAGERY AND GRAPHICS

11. Two of the most common compressed graphic formats are the Graphic Interchange File (GIF) and the Joint Photo Expert Group (JPEG). There are several items to consider

when deciding on which format to use: the type of image you are working with; how small you want your image file to be; and the way you want the graphic to download. Photographs and graphics with lots of colour fields, and particularly colours that blend and fade into one another are best compressed using JPEG. If your image has flat colour fields, it will compress well in the GIF format. It should be noted that GIF compression is limited to 256 colours while JPEG may have millions of colours. JPEG maintains almost complete image quality for photographs and permits a greater degree of compression than GIF, which results in a smaller overall file size. One of the advantages of the GIF format in a web environment is the ability to 'interlace' the image for downloading in a browser. An interlaced GIF appear first with poor resolution and then improve in resolution until the entire image has arrived, allowing the viewer to get a quick idea of what the picture will look like while waiting for the rest. JPEGs can only arrive linearly, from the top row to the bottom row. The other advantage of a GIF is the ability to make the background transparent so that you see the background colour of the browser window you are in. Finally, GIFs can be animated, while JPEGs cannot.

OPTIMIZATION

12. Image file optimization is as important as file compression when attempting to achieve the minimum overall file size and should be used whenever possible. When compressing an image, using GIF or JPEG compression, the physical size of the image is not changed. Images should be resized, cropped, reduced or optimized, for the final intended use or user prior to transmission in a low bandwidth environment.
13. When deciding on the optimum physical size of an image for a web site, information providers must be aware of the designed optimal viewing size of the web site (i.e. 800 x 600) and the proportion of the screen 'real estate' that they intend their image to take when viewed. Imagery should then be optimized for both size and colour depth for viewing in the defined environment.
14. Guidelines on image size should be promulgated in the OPTASK KM. It is acknowledged that requirements may exist to exceed the maximum image file size as laid out in the OPTASK KM in order to transmit very large images for specialized tasks, i.e. photo interpretation by intelligence specialists. Normally, units that have the resources to properly exploit this raw imagery also have a large bandwidth pipe dedicated for this purpose. The results of the fully exploited and processed imagery should then be optimized before being transmitted into the low bandwidth environment.
15. One of the most common tools for optimizing an image size found on almost all Microsoft Windows based PCs, is MS Photo Editor. This tool is standard as part of the MS Operating System. Much more powerful third party imagery editing programs are available, while individual country, user preferences, and procedures should be utilized to optimize imagery size.
16. Third-party tools are available to optimize MS-Office documents such as Word files, Excel spreadsheets, and PowerPoint briefings. These tools can significantly reduce the file size while leaving the file in its native format for future editing. These tools intelligently

resize graphics and eliminate embedded links in the optimization process. For example, MS PowerPoint presentations lend themselves to considerable optimization using the NXPowerLite program.

Uncontrolled copy when printed

MS POWERPOINT

INTRODUCTION

1. PowerPoint is widely employed as a briefing tool. However, the file size of these presentations can become exceedingly large due to sub-optimal default settings and poor practices.

AIM

2. This Annex provides guidance for the preparation of PowerPoint presentations to ensure the file size is manageable and practical for dissemination.

OBJECTIVE

3. The objective is to reduce the size of PowerPoint while not affecting the content. The below diagrams highlight the consequences when these practices are not followed.

DEACTIVATE FAST SAVE

4. Fast Save reduces the time to save a brief by only saving changes, but imposes additional file size overhead. Every time a brief is saved using Fast Save, an additional 7 KB of overhead is added to the file size, regardless of what changes were made.

IMAGES AND PICTURES

5. Images and pictures require significantly greater memory than text. An understanding of how PowerPoint saves these images and pictures, and the application of simple techniques, will reduce the memory requirements for PowerPoint presentations.

6. Picture / Image Utilization – Only images and pictures that are necessary for the clarity of the presentation should be included.

7. Picture / Image Resizing – Reducing the size of an image (i.e. ‘click and drag’ the corner or sides of the image window to resize) will not reduce the file size.

8. Backgrounds – An image as the background for a slide should be avoided. However, colours schemes and fill effects (such as gradient, texture, and pattern) can be employed for presentational effects with little additional memory requirements.

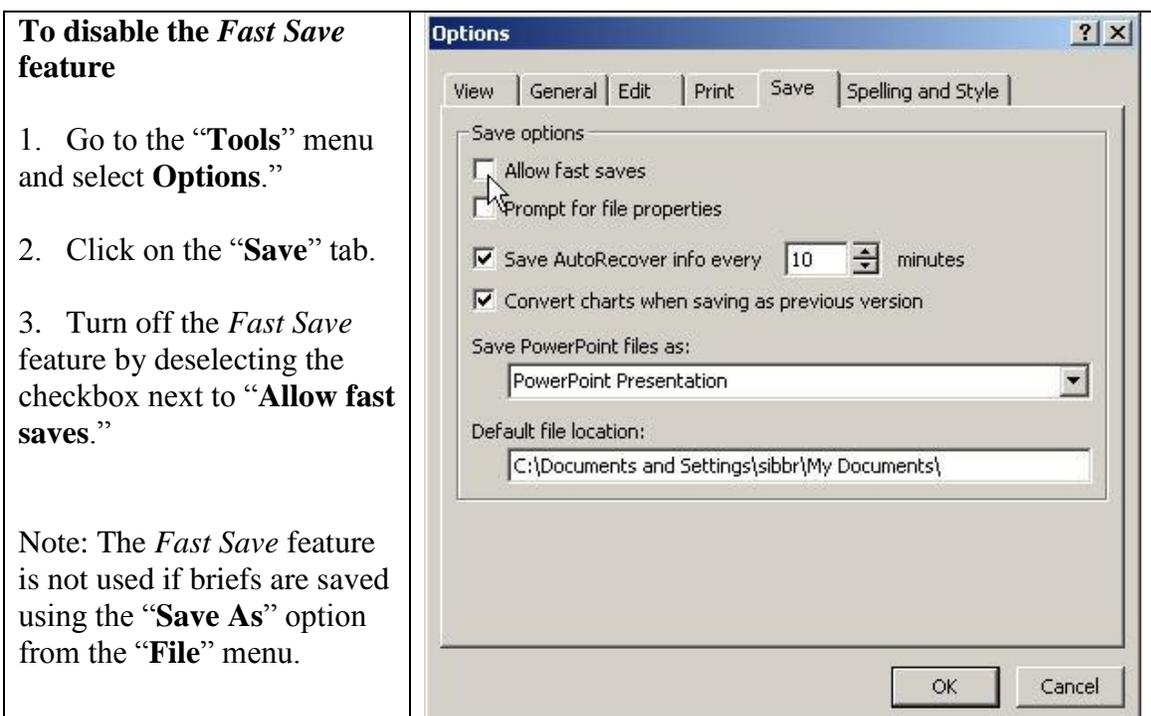


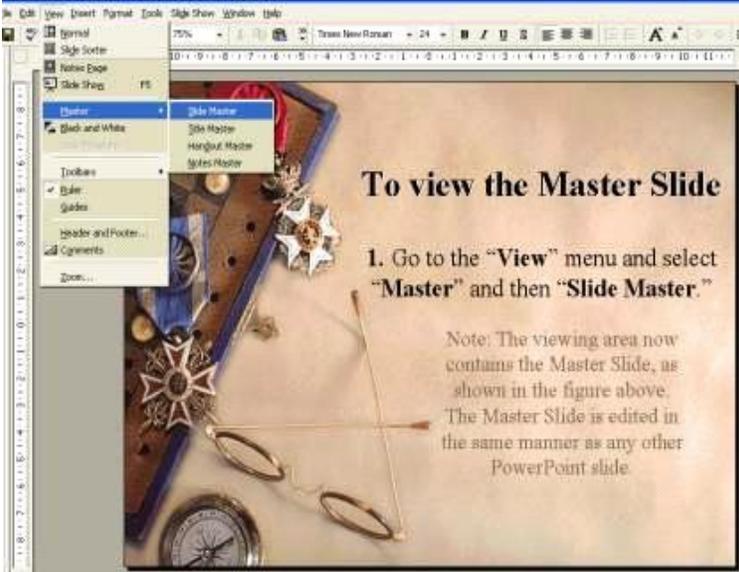
Figure 3-D-1 Fast Save

9. There are a number of methods to reduce the file size of images, including:
 - a. Cropping out background (sky, water, horizon) unless required to “tell the story”;
 - b. Reduce the image size using compacting software (e.g. Microsoft Photo Editor);
 - c. Use .jpeg, .jpg, .png, or other minimizing file formats; and
 - d. Use lower quality images (which are smaller in size).
10. Logos / Unit Insignias should be included only in the Master Slide. If the size of the logo has to be reduced (so that it fits nicely into the corner of a slide) it should be resized in a graphics program, such as Microsoft Photo Editor.
11. There are no additional memory requirements to use different colors or fonts.
12. Bullet types should be set in the Master Slide and not changed in the briefing slides. The cost is about 1 KB for each deviation.
13. Presentations should include the following information within the footer:

- a. Lower Left – DTG of briefing version in local time;
- b. Lower Center – POC information and web posting location; and
- c. Lower Right – Slide Number

MASTER SLIDES

14. Master Slides are used to select the background, fonts, font sizes, bullet type, colors, etc. When these changes are made on individual slides, as opposed to the Master Slide, each change costs several kilobytes of additional space.

	<p>To view the Master Slide</p> <ol style="list-style-type: none"> 1. Go to the “View” menu and select “Master” and then “Slide Master.” <p>Note: The viewing area now contains the Master Slide, as shown in the figure above. The Master Slide is edited in the same manner as any other PowerPoint slide.</p>
--	---

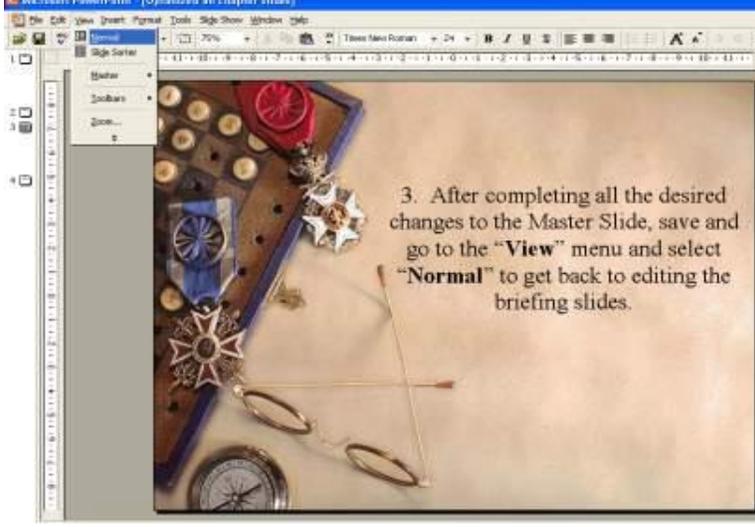
 <p>Click to edit Master title style</p> <p>2. Change the background, font, font size, font colour, bullet types, etc. to whatever is desired.</p> <p>Note: This is where you would insert Unit crests (if desired) for the background.</p> <p>Click to edit Master text styles</p> <ul style="list-style-type: none"> - Second level <ul style="list-style-type: none"> • Third level <ul style="list-style-type: none"> - Fourth level <ul style="list-style-type: none"> • Fifth level 	<p>2. Change the background, font, font size, font color, bullet types, etc. to whatever is desired.</p> <p>Note: This is where you would insert Unit crests (if desired) for the background.</p>
 <p>3. After completing all the desired changes to the Master Slide, save and go to the "View" menu and select "Normal" to get back to editing the briefing slides.</p>	<p>3. After completing all the desired changes to the Master Slide, save and go to the "View" menu and select "Normal" to get back to editing the briefing slides.</p>

Figure 3-D-2 Master Slides

CONCLUSION

15. Although PowerPoint is employed regularly as a briefing tool in operations and exercises, its files may be very large in terms memory size. The size of these presentations can be reduced without affecting the information by following the procedures in this Annex. This promotes efficient employment of the network.

Uncontrolled copy when printed

CHAPTER 4

SECURITY

INTRODUCTION

401. The challenge in a MTWAN is to promote information sharing between allies / coalitions while protecting the information and the information systems that may be logically or electronically connected.

AIM

402. This chapter provides an overview of the security architecture and procedures necessary for a MTWAN.

OVERVIEW

403. For Combined Communications-Electronics Board (CCEB) nations, ACP 122 - Information Assurance for Allied Communications and Information Systems - provides Information Assurance (IA) policies, procedures and doctrine, which enable interconnection and interoperability of IP networks. This chapter applies the policies, procedures and doctrine established in ACP 122 to MTWANs.

DEFINITIONS

404. The following definitions apply:

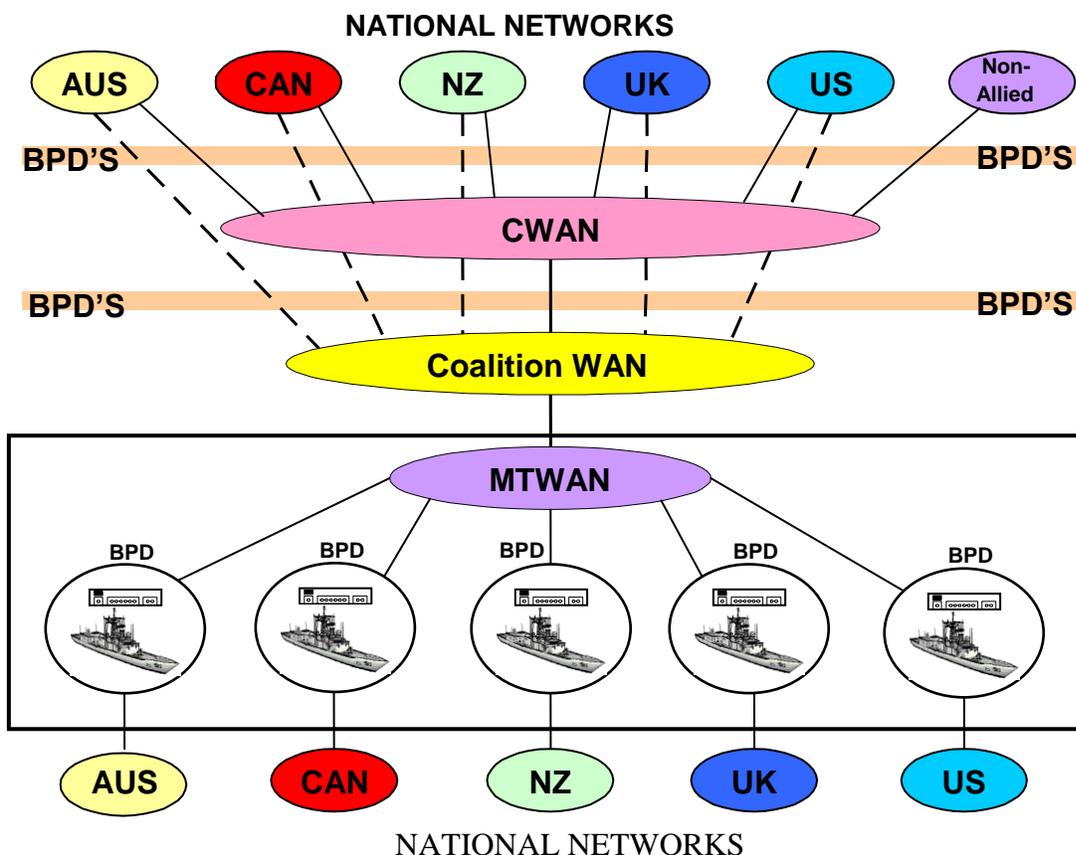
- a. Allied – two or more of the five CCEB nations operating together;
- b. Coalition – one or more of the five CCEB nations operating together with other nations (including NATO);
- c. Joint – two or more of the armed services from one nation operating together;
- d. Combined – joint forces from two or more Allied nations operating together;
- e. Point of Presence (POP) - is an access point from one geographical location to another. A POP may actually reside in rented space owned by the telecommunications carrier to which the Bearer is connected. A POP usually includes routers, digital/analog call aggregators, servers, and frequently frame relay or ATM switches (whatever you need to access the cloud); and
- f. Boundary Protection Device (BPD) – a mechanism that protects the information system and information located on one side of the POP from the other side of the POP.

REFERENCE

405. The principal security reference for any MTWAN is ACP 122. In terms of security policies and procedures this publication is subordinate to ACP 122. Where / if any discrepancies occur, doctrine within ACP 122 should be followed.

NETWORK TOPOLOGY

406. The network topology comprises at a minimum national networks and the MTWAN; the MTWAN being the Local Area Networks (LAN) located in national platforms and connected by RF bearers. More realistically the topology would include connection to an Allied and/or possibly Coalition WAN (CWAN) as represented in Figure 4-1.



NATIONAL NETWORKS
Figure 4-1: MTWAN Topology

Uncontrolled copy when printed

407. Fundamental to the topology is the appropriate separation and security between the national, allied, maritime and coalition domains. Without proper security measures the network will not be accredited for use by respective nations and the Multinational Security Accreditation Board (MSAB).

408. Point of Presence (POP) within this topology exists at the interface of the MTWAN, the CWAN, and to the national networks. The MTWAN domain is treated as a peer-to-peer network, i.e. there are not necessarily protection devices to control access between the MTWAN LANs located on the national platforms. In Figure 4-1, the Allied WAN is also assumed to be part of its peer-to-peer network (this may not always be the case).

409. Boundary Protection Devices (BPD) designed to protect national information system and their information from the CWAN and MTWAN are located before the crypto and POP.

POINT OF PRESENCE / BOUNDARY PROTECTION DEVICES

410. The POP represents the first presence within a sovereign nation that is the ownership and responsibility of that nation (i.e. network passport, terminal adapter, etc., or in other words, it is the first point (box) of a communications bearer). Current management methodologies identify the POP as the line of responsibility for specific security, IT, and accreditation tasks.

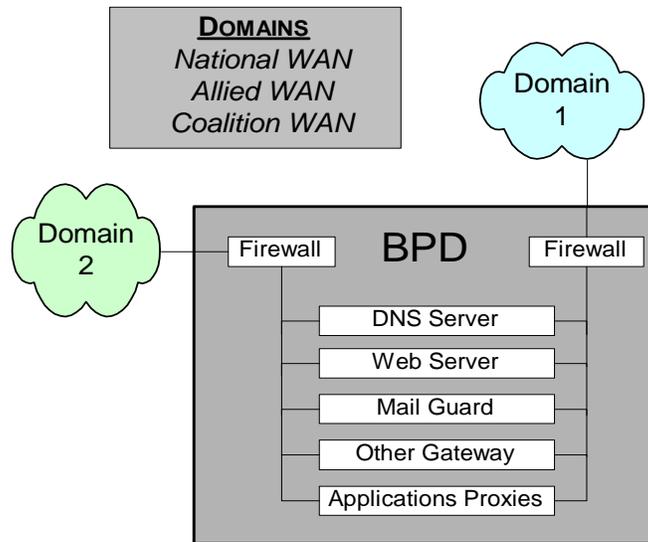


Figure 4-2: BPD Between Domains

411. BPDs are employed behind both the POP and crypto, specifically to provide protection services for the sovereign domain of each participating country. Figure 4-2 illustrates a demilitarized zone (DMZ) where the BPD acts to prevent logical connections

Uncontrolled copy when printed

across domains, but allows the transfer of approved information via a range of services (i.e. DNS, Web, Mail etc).

412. The BPDs may either be an electronic device, a software suite, or a person who generally provides the following functionality:
- a. aGuard - to control the release of information between National, Allied and Coalition networks; and
 - b. Firewall - to protect the National, Allied and Coalition networks against unwanted intrusion.
 - c. Packet-level filtering;
 - d. Address translation;
 - e. Port number filtering; and
 - f. Application proxy.

THREATS

413. Leakage of unauthorized information and penetration by unauthorized users are inherent threats in networks and may result in compromises to the confidentiality, integrity or availability of either the system or the information it contains. These risks are summarized below.

414. Confidentiality – Assurance that information is not disclosed to unauthorized persons, processes, or devices.

415. Integrity – Quality of an IS reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data.

416. Availability – Timely, reliable access to data and information services for authorized users.

417. Accidental Leakage – The system itself or an operator, contrary to the security regulations, releases information inadvertently. A risk exists if the outbound data is transferred unscreened or without label checks, either in real time or off line.

418. Deliberate Leakage – An operator, contrary to the security regulations, releases information. A risk exists if the outbound data is transferred unscreened, either in real time or off line.

419. Stimulated Leakage (Masquerade) – When an attacker pretends to be someone else to stimulate the release of information contrary to the security regulations pertaining to that information.
420. Stimulated Leakage (Trojan Horse) – When malicious software stimulates the release of information contrary to the security regulations pertaining to that information.
421. Corruption of Information (Malicious Code) – When a harmful payload (virus, worm or Trojan Horse) is introduced into a system, either deliberately or inadvertently via the protocol being passed, which corrupts data contained within that system. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.
422. Denial of Service from Malicious Code – When a harmful payload (virus, worm or Trojan Horse) is introduced into a system, either deliberately or inadvertently via the protocol being passed, which prevents the operation of applications or services within that system. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.
423. Denial of Service from Flooding – When applications or services within a system are prevented from operating after its memory devices have been swamped by the introduction of large volumes of data via the inbound leg. A risk exists, however this risk can be reduced by the use of screening software and Intrusion Detection Systems.
424. Spoofing (Masquerade) – Where an attacker masquerades as someone else to distort the view of the reader about the incoming information.

RESPONSIBILITIES

425. Nations have a requirement to protect sensitive and national “eyes-only” information on national networks. The responsibility for the protection of this information resides with the individual nations. Nations will be responsible for ensuring that approved cryptographic devices and IA products (e.g. guards) are employed where required and that national security and COMSEC standards, including key management, are met at all times.
426. Any BPD placed between these national networks and a MTWAN will be nationally owned and controlled. However, the protection of information on a MTWAN itself is the responsibility of the Allied/Coalition participants as a whole. Autonomous System(s) (AS) that leave a MTWAN remain responsible for the continued protection of data that had been externally provided to a MTWAN. This is of particular concern if the AS is to connect to a third party network.

EXPORT SANCTION

427. It is envisaged that BPDs should be able to carry out Export Sanction to guard against accidental and stimulated leakage from the National domain. In addition, BPDs should

provide audit and traceability capabilities to limit the attractiveness of deliberate leakage across the boundary. This function is mandatory in the BPD between a MTWAN/Allied WAN and the CWAN or any other Coalition network. Between a National domain and Allied or Coalition domains, this functionality is entirely the responsibility of the nation concerned.

ASSUMPTIONS

428. The following assumptions are made:
- a. Nations have agreed security principles and tenets;
 - b. Nations have accepted information protection requirements and are working toward a yet to be determined commonality;
 - c. A MTWAN will operate at the SECRET system high level with information releasable to all MTWAN participants;
 - d. All personnel with access to a MTWAN will be cleared to the appropriate level;
 - e. National networks will have been accredited through a mutually agreed process prior to any connection to a MTWAN;
 - f. No connections to National networks will be permitted without passing through a BPD;
 - g. All communications subnets will be protected by High Grade military crypto devices;
 - h. Network nodes are to have appropriate physical, personnel and procedural security measures in place;
 - i. Proposed architectural solutions will not mandate the use of specific applications or products on nations; and
 - j. COTS hardware and software will be used wherever possible.

RECOMMENDED SECURITY ARCHITECTURES

NETWORK CONNECTIVITY

429. An MTWAN will be an AS connected to the Allied WAN through a Network Operations Center (NOC) as shown in Figure 4-3. There are three potential shipboard architectures that have the potential to meet the security requirements. Current technology does not permit the implementation of the integrated solutions; it is intended to migrate to these solutions as technology and policy allows.

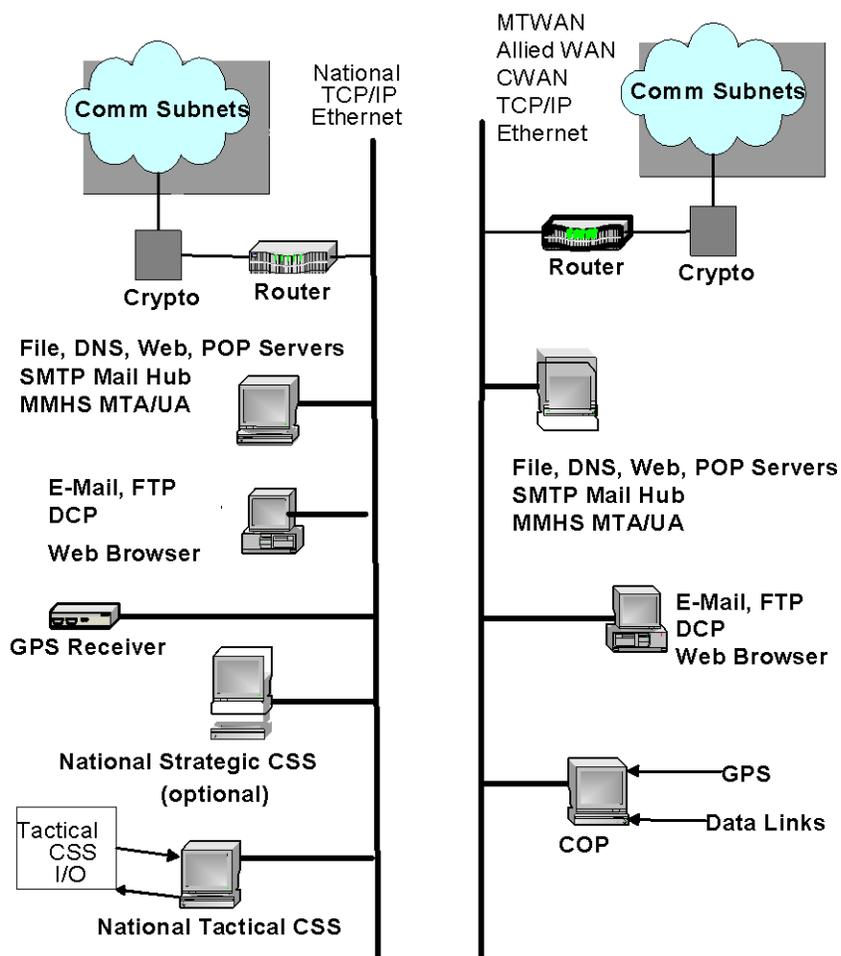


Figure 4-4: Air Gap Architecture

431. By increasing the capability of the security gateway, the duplicate services supported on a MTWAN can be reduced and ultimately eliminated. This will depend on the availability of suitable application proxies and guards devices.

SHIPBOARD “NETWORKED” ARCHITECTURE

432. The ability to exchange information electronically will be required to support the increasing amount of information against the requirement for timely delivery. The architecture shown in Figure 4-5 supports electronic transfers between two networks. Information security will be achieved through a combination of physical, technical and procedural methods.

Uncontrolled copy when printed

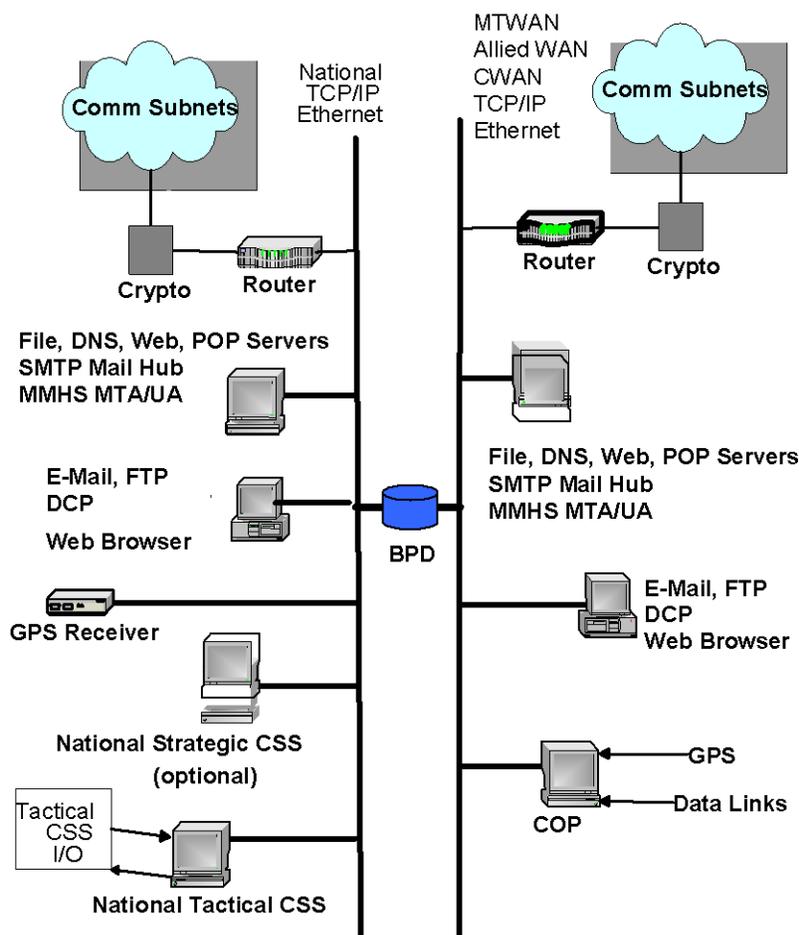


Figure 4-5: Networked Architecture

SHIPBOARD “FULLY INTEGRATED” TARGET ARCHITECTURE.

433. A result of the air-gap and networked solutions is the duplication of resources (e.g. multiple LANs and workstations). This imposes considerable penalties in terms of cost, space and weight. The preferred solution, therefore, is to provide access to both a MTWAN and National networks from a single on-board network.

434. A screened subnet architecture employing both network and application layer firewalls, as shown in Figure 4-6, offers a very high level of protection for the LAN from users on a remote network.

435. Guard devices control and audit all information flowing between the National networks and a MTWAN. They can provide proxy services to users for certain applications (e.g. FTP). The application layer proxy is used to implement virtual connections to application services on the local network. The host may be used to enforce strong authentication on connections from the allied to the national network.

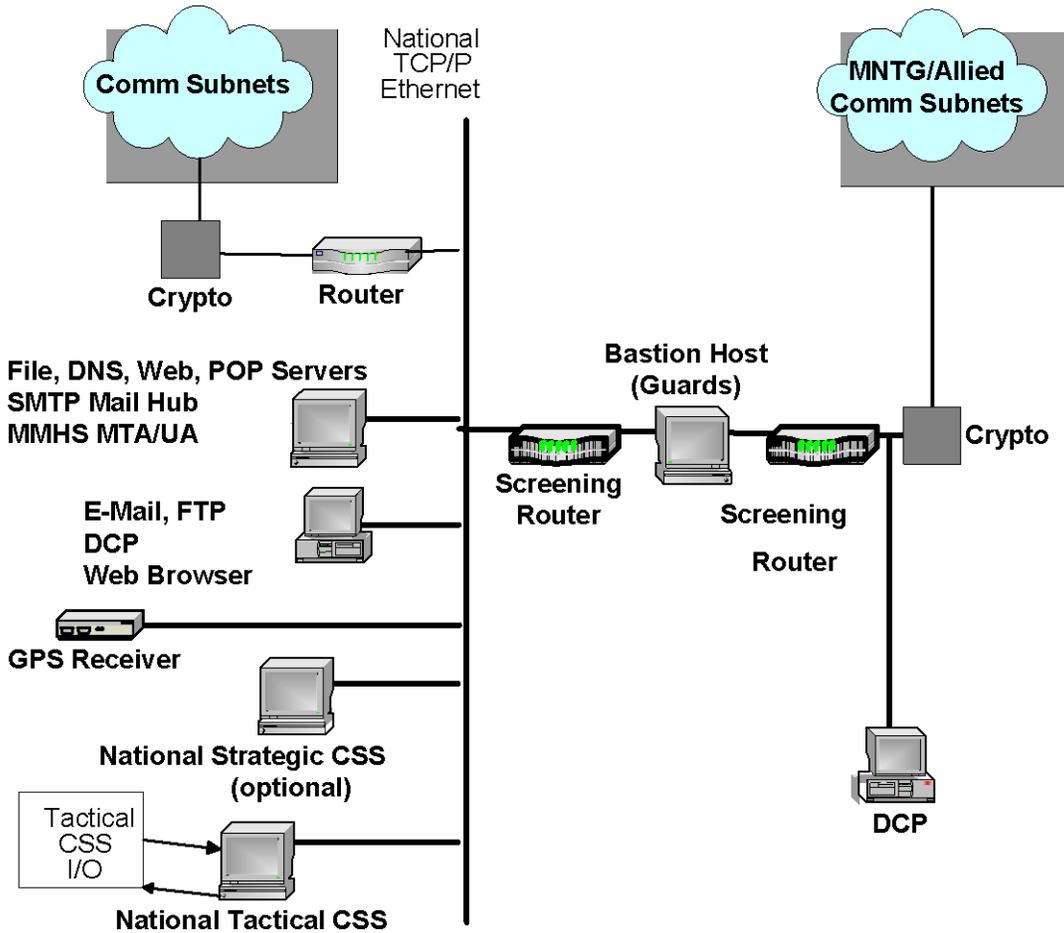


Figure 4-6: "Fully Integrated" Target Architecture

401. Guard devices can also contain application level guard functionality which will control the release of certain information by checking markings and content and, where necessary, by modification to meet sanitization requirements.

402. Servers directly accessible to the Allied/Coalition network will be housed in the screened subnet created between two-network layer screening routers, effectively establishing a network DMZ.

Uncontrolled copy when printed

ACCREDITATION

403. A lead nation will sponsor accreditation of a MTWAN through the Multinational Security Accreditation Board (MSAB).

404. Participating nations will accredit their portion of the MTWAN. Further details can be found in ACP 122.

SECURITY DEVICE INTEROPERABILITY

405. ACP 176 NATO SUPP 1 provides configuration settings necessary to ensure interoperability when different cryptographic devices (e.g. KIV-7/KG84/BID1650) are employed together.

Uncontrolled copy when printed

CHAPTER 5

TRAINING AND INTEROPERABILITY

INTRODUCTION

501. The goal of interoperability is to efficiently share tactical, operational and selected administrative knowledge for planning and executing operations in a coalition environment.

AIM

502. The aim of this Chapter is to delineate common training and an interoperability level for MTWANs.

OVERVIEW

503. Training and interoperability assessment will be a national responsibility. Nations are encouraged to conduct procedure, policy, technical and infrastructure training to support deployed operations.

504. Interoperability level is intended to indicate the operational capability vice only technical connectivity.

TRAINING

505. Training should be focused on network infrastructure and application services to sufficiently allow operators and maintainers to establish, operate, and maintain the network. It is recommended that each nation address the provision of training commensurate to the interoperability level as defined below.

INTEROPERABILITY LEVEL

506. Nations should determine and report interoperability levels to include bandwidth, WAN link capability and supported network services. This will provide the operational commander with common information sets on which to base the OPTASK IM.

DETERMINING INTEROPERABILITY LEVEL

507. A unit's level of interoperability for entering a MTWAN can be determined using the tables 5-1 to 5-3.

508. The following reporting format is to be used: WAN LINK / MINIMUM DEDICATED BANDWIDTH / SUPPORTED APPLICATIONS

WAN LINK	
1.	BFEM-5066
2.	RF IP (Non-SATCOM)
3.	Dial-up Satellite IP
4.	Time Shared Satellite IP
5.	Dedicated Satellite IP

Table 5-1 WAN Link

MINIMUM DEDICATED BANDWIDTH	
A.	Less than 10 kbps
B.	10-32 kbps
C.	33-64 kbps
D.	65-132 kbps
E.	129-256 kbps
F.	257-512 kbps
G.	Greater than 512 kbps

Table 5-2 Minimum Dedicated Bandwidth

SUPPORTED APPLICATIONS	
1 - Essential	Email
2 - Basic	Essential plus Web Browser plus Chat
3 - Advanced	Basic plus at least one of the following – RMP/COP, Whiteboard, VoIP and/or Video over IP

Table 5-3 Supported Applications

REPORTING PROCEDURES

509. Once a unit's interoperability level has been determined it is to be reported up the chain of command IAW national and/or coalition procedures.

Example: A ship leased a 64kbps INMARSAT connection with shared access with another unit. It dedicated at least 20kbps to the MTWAN when connected, using the remaining bandwidth to support national network commitments. The unit is fitted with, and personnel are trained for, the promulgated MTWAN Email, Chat, and Web Browser applications. Using the matrix at Table 5-4, this unit would be referred to as "4B2"

INTEROPERABILITY MATRIX								
DEDICATED BANDWIDTH (kbps)								
WAN LINK	A <10	B 11-32	C 33-64	D 65-128	E 129-256	F 257-512	G >512	NOTES
1. BFEM 5066								
2. RF IP (Non-SATCOM)								
3. Dial-up SATCOM								
4. Time-Shared SATCOM		X						10 hours from 1000Z
5. Dedicated SATCOM								
1 – Essential			2 – Basic			3 - Advanced		

Table 5-4 Interoperability Matrix

Uncontrolled copy when printed

CHAPTER 6

MESSAGING

INTRODUCTION

601. The primary purpose of military communications is to exercise Command and Control over assigned forces. The secondary purpose is to facilitate and expedite the transfer of information between individuals and groups of individuals. Exchange of information can be via traditional military messaging, and more recently email, web-enabled database replication, and chat.

602. Historically, inter- and intra- Task Force / Task Group information transfer was achieved by a variety of low data rate broadcast and point-to-point circuits using formatted messages (ACP 127 etc). Increased information transfer resulted in traffic backlogs, delays, and non-delivery during periods of high intensity operations. During the 1991 Gulf War, a single day's message traffic surpassed the total Allied messages exchanged during the whole of the Second World War.

AIM

603. This chapter provides guidance for the employment of messaging within a maritime IP network.

OVERVIEW

604. ACP 127/128 provides many Elements of Service (EoS) that support Command and Control over assigned forces. These EoS, or key features, include precedence handling, Plain Language Address Designator (PLAD), and distribution by subject.

605. A principal limitation of ACP 127/128 messaging is that it does not support a wide variety of characters, symbols, case formats, font styles, sizes and color, or the inclusion of attachments. As such, traditional messaging does not support multimedia formats.

606. Email provides rich text formats (i.e. a variety of fonts, styles, characters, and symbols) in addition to allowing the drafter to send a message to a reader without any intermediaries. This latter aspect is referred to as 'writer-to-reader' messaging. A significant benefit of email over traditional messaging is the speed at which information can be exchanged.

607. Chat provides the capability to exchange short instantaneous text messages with an individual, or individuals, over an IP network.

608. Web-enabled database replication offers an efficient alternative to formal message traffic by enabling information previously encapsulated in formal messages to be posted to a

database for access by “addressees” on a “pull” basis in a multimedia format. This places the emphasis upon the “action addressee” to retrieve the information posted vice the traditional “push” mechanism of formal messaging circuits.

609. Commanders should select the appropriate method for messaging dissemination taking into consideration the relative limitations of text based messaging (and its Elements of Service (EoS) benefits), versus the richer attributes of multimedia messaging formats.

610. Multicast messaging techniques offer a more efficient method of messaging over a bandwidth-constrained network than current “unicast” methods.

611. Public Key Infrastructure (PKI) may offer EoS (authentication and non-repudiation) to multimedia messaging systems.

TYPES OF MESSAGING

612. Messaging can be either text-based or multimedia formats. ACP 127/128, OTH-GOLD, and Chat messaging are text-based while email and Web services support a multimedia capability. ACP 123 (when implemented) will support message integrity, message confidentiality, non-repudiation, and authentication. Robust and reliable messaging protocols and services should be used in order to reduce network congestion.

TEXT-BASED FORMATS

613. As noted above, ACP 127/128 provides many EoS (e.g. precedence handling, Plain Language Address Designators (PLAD), and distribution by subject) that support Command and Control over assigned forces. It was also noted that a principal limitation of ACP 127/128 messaging is its lack of support for characters, symbols, case formats, font styles, sizes and color, and the inclusion of attachments. As such, traditional messaging does not support multimedia formats. EoS such as message integrity, message confidentiality, non-repudiation, and authentication provide greater assurance in the exercise of command and control, i.e. the primary purpose of military communications. Currently, EoS is only provided by ACP127/128 text based messaging systems.

CHAT

614. Text chat is increasingly being used to support Command and Control during operations. Chat provides the capability to provide short instantaneous text messages with an individual, or group, over an IP network. Chapter 9 (Distributive Collaborative Planning (DCP)) provides further guidance on the use of chat.

MULTIMEDIA FORMATS

615. The ability to send email and replicate web-enabled databases within a Task Group enhances traditional methods of information transfer. Email and web-enabled database replication over Local and Wide Area Networks (LAN / WAN) have been shown to:

- a. Improve the timeliness of information delivery;
- b. Reduce message traffic congestion;
- c. Improve the information richness of the message by use of multimedia attachments; and
- d. Increases the demands on staff to monitor multiple information sources.

E-MAIL

616. Email provides rich text formats (i.e. a variety of fonts, styles, characters, and symbols), in addition to allowing the drafter to send a message to a reader without any intermediaries. This latter aspect is referred to as ‘writer-to-reader’ messaging. A significant benefit of email over traditional messaging is the speed at which information can be exchanged.

WEB SERVICES

617. The ability to post a message such as the Air Tasking Order (ATO) or general operational messages (OPGEN) to a Task Group Web Page reduces the amount of Broadcast Messaging (Multi-cast email and ACP 127/128 messages) to be sent across a network. Through the use of replication logs, database replication provides increased information traceability, authenticity, and integrity over non-replicated systems. Chapter 8 provides further guidance on the use of Web Services for information exchange.

618. Within a tactical WAN, messages posted to web pages have replaced traditional broadcast messages as the most efficient mechanism for disseminating signals, such as Daily Tasking, Operational Reports (OPREPs), ATOs, Operational Tasking messages (OPTASKs), and OPGENs that are promulgated on a regular basis. The fact that this information must be pulled from a web site by users must be taken into consideration by the promulgator. Information posted in this manner requiring response or action would normally require action addressees to acknowledge receipt of the information by another mechanism such as military messaging, email or chat.

619. Web replication offers an efficient alternative to formal message traffic by enabling information previously encapsulated in formal messages to be posted to a database for access by “addressees” on a “pull” basis in a multi-media format. This places the emphasis upon the “action addressee” to retrieve the information posted vice the traditional “push” mechanism of formal messaging circuits.

MESSAGING SELECTION

620. Commanders should select the most effective method of transferring information, being cognizant of all the issues outlined in this chapter. Furthermore, Commanders should provide guidance with regard to the messaging method used for operational direction. This

guidance should be promulgated in the OPTASK Information Management (IM) (See Chapter 3 Annex B).

621. Until an ACP 123 capability is fully adopted, there will be a requirement to duplicate some information via ACP 127/128. Careful consideration, and a clear understanding of, the information that must be supplemented by ACP 127/128 messages can minimize this duplication.

622. The OPTASK IM should promulgate the authorized methods for executing command and control. Table 6-1 provides guidance in this area

MULTICAST MESSAGING

623. This document describes the employment of SMTP and add-on-services as an interim solution for an IP based messaging service.

624. Multicast messaging allows the same message to be sent to several message servers simultaneously, rather than the generation of a separate copy for each addressee.

625. Standard SMTP email uses Transmission Control Protocol (TCP). In instances when a single message is being delivered to several recipients that are served by different Message Transfer Agents (MTAs), standard SMTP email must establish a connection and transfer the message to each of the destination MTAs in turn. This is very inefficient, as the same message must be transmitted several times, once for each destination MTA, consuming considerable network bandwidth. To resolve this inefficiency, P_MUL was developed to take enable multicasting. The MTA can be configured to deliver SMTP mail using the P_MUL protocol. P_MUL also supports the use of email during periods of emission control (EMCON), by allowing SMTP email to be sent with a delayed acknowledgement. Other transport mechanisms such as MSeG, which multicasts GOLD messages, and MCHAT (Multicast Chat) provide similar efficiencies.

Information Transfer Application	Authentication	Non - Repudiation	Message Confidentiality	Message Integrity	Recommendations
ACP 127/128	Yes	Yes	Yes	Yes	Use for brevity to authenticate all operational tasking. Priority and delivery is guaranteed. Provides redundancy for tactical WAN
Email	No	No	No	No	Delivery not guaranteed. Operational direction sent by email should be supplemented by formal message
Email with digital signature	Yes	Yes	No	No	May be considered for transfer of operational direction without formal message backup but delivery is not guaranteed. Provides proof of originator's identity and confidence to act on direction. Not needed for admin traffic.
Email with digital signature & public key encryption	Yes	Yes	Yes	Yes	May be considered for transfer of operational direction without formal message backup but delivery is not guaranteed. Provides proof of originator's identity, confidence to act on direction, confidentiality and confidence in the accuracy of the message Not needed for admin traffic.
Text Chat	No	No	Yes (secure net)	No	Can be used for tactical direction provided that the Commander can guarantee that all units are on the net.
Text Chat with encryption	Yes	Yes	Yes	No	Chat products are available that provide 128 bit encryption.

Uncontrolled copy when printed

Information Transfer Application	Authentication	Non - Repudiation	Message Confidentiality	Message Integrity	Recommendations
GOLD (Opnotes)	No	Yes	Yes (secure net)	No	Suitable for the exchange of tactical information but not direction.
Web Page Messaging	No	No	Yes	No	Suitable for administrative information only
Web-enabled database Replication (Webpage Messaging with replication)	Yes	Yes	Yes	Yes	Suitable for commonly promulgated Orders and Schedules. Acknowledgment by action addressees required.
Web-enabled Replication with PKI	Yes	Yes	Yes	Yes	Suitable for commonly promulgated Orders and Schedules. Acknowledgment by action addressees required. PKI provides extra assuredness in Authentication and Non-repudiation

Table 6-1 Messaging Selection

626. The importance of bandwidth efficiency cannot be understated. An SMTP mail transmission typically involves 19 exchanges of data in addition to those required to transmit the message. These exchanges add up to 1100 bytes. The SMTP mail message typically contains approximately 400 bytes of message headers generated by mail user and mail transport agents. A single email of 1000 bytes therefore requires about 2500 bytes to be transmitted in 20 exchanges. Any measure that reduces the number of emails, such as posting information to the web for replication, is therefore advantageous.

PUBLIC KEY INFRASTRUCTURE (PKI)

627. PKI can be used within email services to provide an element of military assuredness. By using public key encryption and a digital signature, authentication and non-repudiation can be guaranteed.

628. Use of a digital signature and/or encryption of email messages is not always needed or recommended. When used, these features will typically increase the email overheads by 3 to 9 KB. There is currently no stated requirement for public key encryption for any secure military network.

CONCLUSION

629. The primary purpose of military messaging remains to support Command and Control. Alternative methods are now available that significantly enhance the ability and flexibility of Commanders to pass information. It is important that Commanders promulgate the messaging options that they intend to use for operational and administrative traffic.

Uncontrolled copy when printed

STANDARD DEFINITIONS FOR MILITARY MESSAGING

INTRODUCTION

1. The following military messaging definitions have been taken from various ACPs and policy documents in order to provide a consolidated list for ease of users of the ACP200.

MESSAGE INTEGRITY

2. This provides a method of ensuring the content that was received is the same as that which was sent by the originator.

MESSAGE CONFIDENTIALITY

3. This protects against unauthorized disclosure of the message.

DATA ORIGIN AUTHENTICATION

4. This provides assurance that the message was originated by the user indicated as the sender.

ACCESS CONTROL

5. This validates authorization of the user originating and receiving messages. Access control implementation details are a national matter and local to the user. Messages both sent and received shall not violate the security policies of the originators and recipients.

MESSAGE NON-REPUDIATION WITH PROOF OF ORIGIN

6. Non-repudiation provides the recipient with evidence that demonstrates, to a third-party, who originated the message, and will protect against any attempt by the message originator to falsely deny having sent the message. This evidence is the proof of origin of the message, which effectively is a digital signature and the certificates necessary to verify it. The digital signature for the message must not be affected by subsequent revocations of the originator's certificates. Preservation of evidence and additional records management procedures must also be applied.

CHAPTER 7

COMMON OPERATIONAL PICTURE (COP)

INTRODUCTION

701. Situational awareness is of vital importance to both warfighters and Commanders in that it enables them to make more-informed decisions. The COP provides a Commander the ability to see, at a glance, the true disposition of all forces and ships within his/her area of interest. Thus the COP is an essential decision-making tool and a force multiplier.

702. Within a MNTG, tactical situational awareness can be provided from data/information received from organic sensors being captured and displayed on combat data systems. However, this data, while real-time, is limited in coverage to the extent of the TG/TU dispositions and their sensor capabilities. On the other hand, the COP provides near real-time information to the Commander from a theatre-wide perspective. This picture is often enriched from information sources external to a MNTG, and includes land and air tracks.

AIM

703. This chapter describes the COP and its dissemination in a MTWAN environment.

OVERVIEW

704. The COP is an amalgamation or fusion of data and information from a number of combined and/or joint sensors, data-links and other sources into a single (or common) operational picture. The COP provides Near-Real Time (NRT) (current, planned or projected) disposition and amplifying information on friendly, hostile, neutral and unknown forces / units in the sea, land, air and space environments through a Graphical User Interface (GUI).

705. Other products such as imagery, mapping and weather / oceanography may be overlaid. Ideally future information such as force status, logistic, and intelligence is integrated to increase the overall value of the information. This information is either in the form of overlays or can be 'pulled down' by opening windows; (providing a 'drill-down' capability).

706. At the tactical level, access to the COP augments situational awareness while at the operational and strategic levels it provides an authoritative picture or theatre-wide overview. Traditionally the COP has been disseminated to maritime forces through satellite Information eXchange Sub-Systems (IXS) or via a High Interest Tracks (HITS) broadcast. Both are inefficient and costly to support because they are 'stovepipes' that require dedicated subnets. New COP dissemination techniques employing Internet Protocol (IP) allow the convergence of COP information onto the one maritime tactical network. These IP COP methods provide for the more timely delivery of track information.

REQUIREMENT

707. It is essential a Commander has confidence in the COP, and therefore willing to act on the information displayed. To this end, the information must be:

- a. Accurate – it must convey the true situation;
- b. Relevant – it must apply to the mission, task, or situation at hand;
- c. Timely – it must be received in time to make the right decisions;
- d. Useable – it must be in easy to understand, format and displays;
- e. Complete – it must contain all the information necessary to make an informed decision;
- f. Concise – duplicate and superfluous information should be avoided;
- g. Secure – it must be afforded adequate protection; and
- h. Common – data and tracks must be identical across the theatre.

TOP COP (FUSION AND FILTERING)

708. The TOP COP denotes a hierarchical architecture where information is fused (merged, enriched, correlated and if necessary de-conflicted) from subordinate pictures so that the ‘TOP COP’ has a fully integrated and accurate picture. This is then fed back down to subordinate pictures, which are updated. The COP Synchronization Tool (CST) seamlessly provides much of this capability, to sites that have sufficient bearer bandwidth. The use of a Force Over-the-horizon Track Coordinator (FOTC) ensures COP fusion at the tactical level where CST is often not available.

709. At the tactical level, an important requirement is to ensure relevancy. This also adheres to IM principles and requires coordinators to be able to filter unwanted information captured at operational and strategic levels. The principle here is “keep it relevant”. It is unlikely that a tactical Commander needs information from outside of his area of interest.

COP MANAGEMENT

710. The COP is a distributed fused picture. In order to achieve a “synchronized” fused picture with multiple units that may all be reporting similar pictures a method of synchronization is necessary. Traditionally this has been accomplished procedurally by the designation of a FOTC who maintains responsibility for all tracks within the AOR. The COP Synchronization Tool (CST) provides a “distributed” rather than “dictated” management of the database. There are three methods of COP Management as follows:

FOTC

711. Traditional COP management has been achieved through the establishment of a FOTC, which correlates and associates, where possible, the various source track data and then provides a “dictated and validated” broadcast back to the participants. The validated track database is centrally managed and maintained within the TF/TG.

CST

712. CST enables the unit that has the most information on a particular track with the ability to be the one responsible for managing that track within the database. Based on TCP/IP communication protocols, CST provides the user with faster, more reliable communications and an improved synchronized picture.

DUAL FOTC / CST

713. In many cases there are requirements to support both CST and FOTC. A CST / FOTC Gateway platform enables units within a TF/TG to receive the benefits of a CST fused picture.

COP DISSEMINATION**CSTMdxNET / CST**

714. CSTMdxNET is the transport protocol associated with CST. It enables the transmission of COP track data via TCP/IP. The minimum recommended bandwidth to participate in a CST environment is 40 kbps. Platforms not meeting these bandwidth criteria should continue the use of the traditional FOTC-based broadcast.

UNIT IDENTIFIER (UID)

715. UID is a TCP/IP transport protocol that enables the transmission of Over The Horizon (OTH) Gold Formatted messages. This requires less oversight than OTCIX/HITS/FOTC Broadcast and yields greater commonality in the database. Within a maritime tactical WAN environment the use of UID is the simplest mechanism for COP distribution but carries a large overhead because the dissemination is unicast.

NETPREC

716. NETPREC is subset of UID that enables FOTC to group units for dissemination of tailored COP. NETPREC is designed for LAN application and is seldom used within a WAN environment.

MULTICAST TRANSPORT SERVICE

717. See Chapter 13

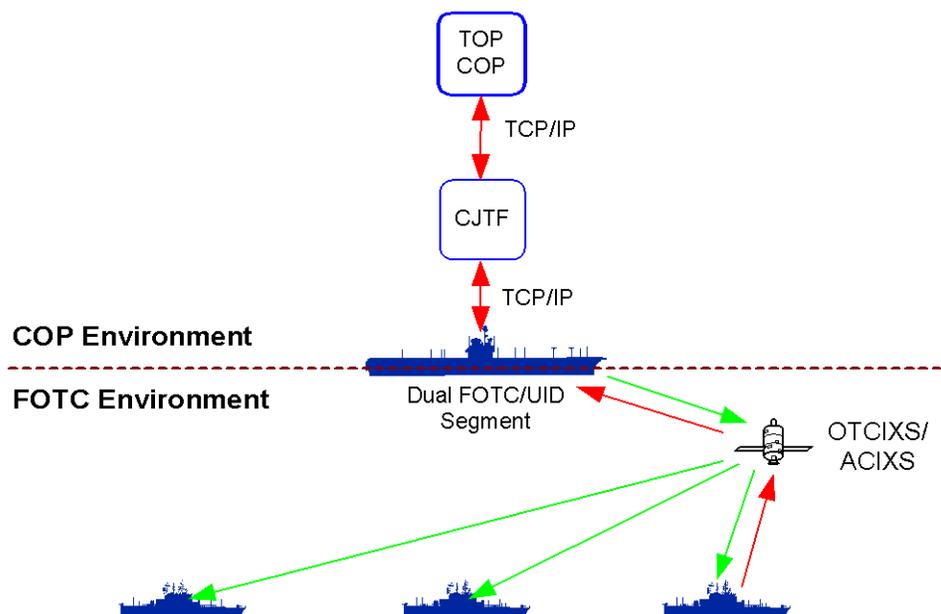


Figure 7-1 Traditional Environment (with IXS networks and CST)

COP ARCHITECTURE

718. Figures 7-1 and 7-2 provide the generic architecture for the generation and distribution of the COP. They show both a top-down and bottom-up approach in that strategic and theatre information is assimilated and passed downwards at the shore NOC, while a force picture is generated and passed upwards.

719. Figure 7-2 represents a full IP environment with CST operating upwards from the MCC and subordinate units participating via MSeG or UID.

720. The World Wide OPTASK Force Over-the-Horizon Track Coordinator (FOTC) provides detail on construction, compilation, collation and dissemination of the COP. CTF will promulgate variations in COP procedures specific to local operations in an OPTASK FOTC Supplement.

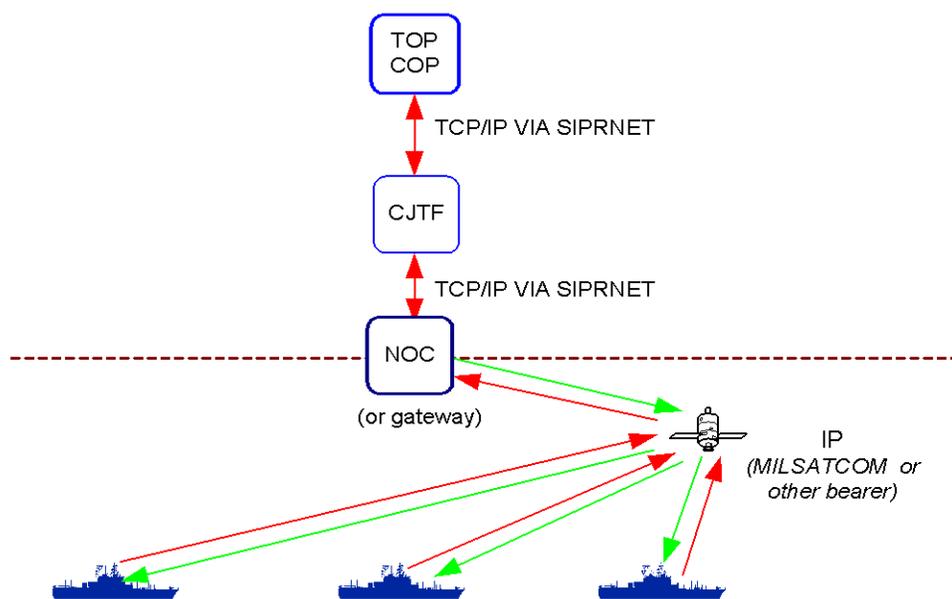


Figure 7-2 Full IP Environment (MTWAN)

SELECTION OF APPROPRIATE COP DISSEMINATION METHOD

721. The following table provides guidance for the selection of COP dissemination.

Method	Transport Service	Description	Considerations
CST	CSTMdxNET	1. Reporting responsibility assigned to unit with best track information. 2. Synchronized track databases 3. Automatic process 4. Utilises TCP/IP	1. Not recommended unless WAN bandwidth 64Kbps or greater 2. Can be employed with 20 Kbps bandwidth with degradation in service (i.e. functionality)
FOTC	UID	1. Maintains FOTC procedures 2. Dictated and validated COP 3. Simple and efficient Utilizes TCP/IP	1. Point to Point
FOTC	MSeG	1. Packet assembler enabling multicast of COP via TCP/IP 2. Has a Broadcast mode	1. FOTC procedures unclear 2. Higher track latency 3. Can be utilized in EMCON

Uncontrolled copy when printed

Method	Transport Service	Description	Considerations
FOTC	IXS	1. Maintains FOTC procedures 2. Dictated and validated COP 3. Has a Broadcast mode 4. Legacy system	1. Dedicated stovepipe system (independent of network traffic) 2. Higher track latency 3. Can be utilized in EMCON

Table 7-1 COP Dissemination Methods

CONCLUSION

722. The COP is a vital tool for improving the Commander's situation awareness and aiding in decision-making. However, the COP is only as good as the information fed into it and, conversely, could seriously damage situational awareness if allowed to become out of date or contain inaccurate, irrelevant or incomplete data. In fact, an inaccurate picture is worse than *no picture at all* because it can cause the wrong decisions to be made, possibly with devastating results. Consequently, a Commander will have confidence in the COP *only* if he/she knows that the system is reliable and accurate. This can only be achieved through users being knowledgeable, aware of the system requirements and diligent in its upkeep.

723. The ability to display global track information through stovepipe IXS networks will soon be replaced by integration onto IP networks. This will allow the COP to be displayed and viewed through a variety of media that will continue to provide a picture, even during EMCON restrictions (radio silence). Conversely, it also means that units that are not IP capable and do not have access to the MTWAN may not be able to view the same picture within the same timeframe. Commanders must therefore be aware of the capabilities and limitations of the units within their force.

Combined Requirements for COP

Tier 1 JCA : Joint Command and Control (JC2)		
Tier 2 JCA : Situational Understanding/Common Operational Picture		
Task : 2.4 Provide Operational Intelligence, Surveillance, and Reconnaissance (Op 2.0)		
Sub-tasks	Attributes	Standards
2.4.1 Plan battlespace awareness/ISR operations (A2.3.2)	Accessible	3 steps or less required for a user to gain access to data and information services.
	Sufficient	90% of nodes requesting service receive it.
2.4.2 Manage collection/intelligence requirements (A2.3.2.4.2.1 and Fn 1.6)	Accessible	90% of nodes able to publish/subscribe. 10% saturation of communication channels.
	Compatible	100% of types of nodes able to publish/subscribe.
		45,000 users publish or subscribe information. (NECC Standard)
	Sufficient	95% of collected information is received.
		90% of number of data packets requested are delivered.
		100% of data throughput maximized.
Timely	8 seconds required to publish or subscribe information, by node. (NECC Standard)	
Usable	45,000 users publish or subscribe information. (NECC Standard)	
Task : 2.5 Assess Operational Situation (Op 5.2)		
Sub-tasks	Attributes	Standards
2.5.1 Maintain a 24/7 intelligence and warning watch (Op 5.1)	Complete	95% of pertinent sources used.
	Flexible	95% of types of data can be fused.
	Structured	100% sources identified in fused data.
	Timely	8 seconds required to fuse new data with existing, by data type. (NECC Standard)
2.5.2 Collaboratively develop shared understanding of regional/local factors	Coherent	90% of personnel receive necessary guidance and act in accordance with that guidance 90% of the time. (C2 JIC 6.2)

Uncontrolled copy when printed

(A.3.4.6.4.2 and C2 JIC 6.2)	Accurate	100% of critical mission/operational requirements are reflected by appropriate operations standards.
2.5.3 Provide the means for decision makers to interact in the comparison and assessment of shared plans, visualizations, work (2.5.3 cont) products or other information objects in order to reach mutual understanding (Fn 7.2)	Assured	90% of information products provided for collaboration include their source and validity.
		100% of sources used and development history available for products.
		100% of collaboration products include visual ID of their contributors.
	Flexible	1500 users can synchronously or asynchronously contribute to the creation of a work product. (NECC Standard)
		10 unique types of products can be used in collaborative sessions.
Timely	90% of work products are available to other users in time to meet their deadlines.	
	Maximum of 5 seconds between product posting and availability for collaboration.	

Task : 2.6 Receive, Process, and Display Information, Provide Tasking and Support Decision-Making (Seabasing JIC and A.2.4)

Sub-tasks	Attributes	Standards
2.6.1 View tailored relevant situational information (A2.4.4)	Compatible	5% of required data elements missing in a representation, by visual representation type.
		Subjective determination of degree to which a visual representation meets the requirements of each user, by user (1-5 scale: 1 fully met, 5 not met).
	Flexible	100% of information can be represented by visual modes or forms.
		100% of required visual representations can be simultaneously displayed.
		100% of required user defined specialized representations are available.
Usable	Maximum of two requests for clarification of a visual representation, by representation type.	
	Maximum of two steps required to switch from one representation to another.	
2.6.2 Task for collection/production (A2.3.2.5 and C2 JIC 1.4/1.8/4.7)	Coherent	100% of a group or team's products match or meet unit and individual mission goals to further the commander's intent. (C2 JIC 1.4)
	Flexible	100% of mission critical decisions can accommodate effective responses that facilitate task change without detracting from the primary mission. (C2 JIC 4.7)
	Foresight	Significant risks are anticipated 90% of the time. (C2 JIC 1.8)
	Suitable	100% of benefits of successful effect outweigh impact of potential risks. (C2 JIC 1.8)
2.6.3 Resolve ambiguities in	Assured	90% of redundant data (tracks) can be eliminated through correlations

Uncontrolled copy when printed

understanding of the situation (A3.4.6.4.3.1 and Fn 5.5)		95% of resultant tracks have correct ID after deconfliction.
	Capable	100,000 information/tracks can be deconflicted. (NECC Standard)
	Effective	90% of cases can be deconflicted.
	Flexible	100% of presentations can be accomplished with deconflicted information.
	Sufficient	90% of multiple sources deconflicted.
	Timely	95% of the time to deconflict multiple reports in less than 8 seconds.
2.6.4 Develop and maintain shared awareness of the situation (A2.5 and Fn 15.2)	Usable	Subjective determination of usability of deconflicted information (fully, marginal, unusable).
		5% of tracks have lost needed information during deconfliction.
	Assured	100% of presented options were considered.
		Appropriate number of SMEs consulted in decision-making (situation dependent).
	Flexible	100% of branches and sequels are available for plans requiring them.
		Time permitting, 95% of courses of action war gamed against projected threats. 95% of options considered.
	Sufficient	95% of forces needed for the operation are provided direction.
		Complete order-of-battle descriptions (complete, partially, insufficient).
	Timely	6 hours to develop course(s) of action from time of warning/tasking.
		60 minutes to approve a course of action after development.
15 minutes for decision with respect to current force deployment.		
Task : 2.7 Manage Sensors and Information Processing (A2.3)		
Sub-tasks	Attributes	Standards
2.7.1 Plan battlespace awareness/ISR operations (A2.3.2)	Accessible	3 steps or less required for a user to gain access to data and information services.
	Sufficient	90% of nodes requesting service receive it.
2.7.2 Establish information management business practices that support organizational processes (Fn 1.3)	Accessible	90% of nodes able to publish presence/identity and offer available services.
		90% of provided services available, by requesting node.
	Manageable	Less than 15 minutes required to make services available after request, by service.
2.7.3 Communicate operational information (Op 5.1.1)	Sufficient	95% of required services available on the network.
		Assured
		95% of reports for which unit identity can be confirmed as correct.

Uncontrolled copy when printed

	Sufficient	90% of nodes have accurate, current location information.	
		100% of required types of nodes able to report.	
		100% of required status dimensions reported by any node.	
	Timely	90% of units reporting.	
		Information is updated every 5 seconds.	
2.7.4 Manage means of communicating operational information (Op 5.1.2 and Fn 7.1)	Accessible	90% of nodes update within established timelines.	
		3 steps or less required for a node to access a product, by product.	
		98% of on-line nodes can post and share their products. (NECC Standard)	
	Extensive	45,000 users can share an information product at one time. (NECC Standard)	
		90% of information products can be shared among nodes.	
		100% of types of information products can be shared among nodes.	
	Manageable	90% of nodes can share an information product at one time.	
		100% able to visually relate information in products from different nodes	
	Structured	100% able to visually highlight the information product from a node for use in the collaboration.	
		100% of information packages can be visually related to the node that provided them.	
	2.7.5 Maintain operational information and force status (Op 5.1.4 and Fn 2.1)	Assured	100% of required horizontal and vertical geolocation accuracy reported in x, y, z coordinates. (NECC Standard)
			95% of reports for which unit identity can be confirmed as correct.
90% of nodes have accurate, current location information.			
Sufficient		100% of required types of nodes able to report.	
		100% of required status dimensions reported by any node.	
		90% of units reporting.	
Timely		Information is updated every 5 seconds.	
		90% of nodes update within established timelines.	
2.7.6 Monitor battlespace for dynamic events (Detect) (A2.3.3.1.8)		Assured	Reconnaissance and surveillance available for 95% of AO.
	90% of reconnaissance/surveillance missions conducted in accordance with assigned parameters.		
	Sufficient	Required rate of area surveillance available (situation dependent).	
		95% of targets located within allocated on-location time.	

Uncontrolled copy when printed

	Manageable	100% of assets available to obtain required information, by info type.
		90% of info types for which capture means are available and can be tasked.
	Timely	8 seconds since latest information published. (NECC Standard)
		5 minute gap in coverage of a given target.
		15 minutes required to locate target area.
		60 minutes required to locate target once sensor scans appropriate area.
		60 minutes since meteorological data updated.
		60 minutes since oceanographic data updated.
		15 days since geospatial data updated.
		Rate of synchronization updates between units is 12 times per minute. (NECC Standard)

Tier 1 JCA : Joint Net-Centric Operations

Tier 2 JCA : Technical Connectivity

Task : 5.1 Maintain Operational Information and Joint/Naval Force Status (A2.4 and JFEO JIC)

Sub-tasks	Attributes	Standards
5.1.1 Manage COP (A2.4.1)	Flexible	More than one type of information available to support user defined environments. More than one view available to support user defined environments.
	Manageable	3 steps or less required for a user to gain access to data and information services.
5.1.2 Assess COP information (A2.4.2)	Extensive	95% nodal connectivity.
	Timely	8 seconds between product posting and availability for collaboration.
5.1.3 Collate COP information (A2.4.3)	Extensive	95% nodal connectivity.
	Timely	8 seconds between product posting and availability for collaboration.
5.1.4 Establish collaboration structures and processes across the force (A3.2.1.2.1.6)	Extensive	95% nodal connectivity.
	Timely	8 seconds between product posting and availability for collaboration.
5.1.5 Develop an MHQ C2 structure (A3.2.1.2)	Extensive	95% nodal connectivity.
	Flexible	More than one type of information available to support user defined environments. More than one view available to support user defined environments.

Uncontrolled copy when printed

	Manageable	3 steps or less required for a user to gain access to data and information services.
	Timely	8 seconds between product posting and availability for collaboration.

Uncontrolled copy when printed

Tier 2 JCA : Shared Knowledge, Understanding, and Collaboration

Task : 5.8 Develop a Shared Understanding of the Situation (A3.4)

Sub-tasks	Attributes	Standards
5.8.1 Each node publish extensive operational/mission-oriented information on itself - such as location, status, plans or intentions (Fn 2.1)	Assured	100% of required horizontal and vertical geolocation accuracy reported in x, y, z coordinates. (NECC Standard)
		95% of reports for which unit identity can be confirmed as correct.
		90% of nodes have accurate, current location information.
	Sufficient	100% of required types of nodes able to report.
		100% of required status dimensions reported by any node.
		90% of units reporting.
Timely	Information is updated every 5 seconds.	
	90% of nodes update within established timelines.	
5.8.2 Identify, calculate, report and update positions of friendly units, elements or entities that are not able to function as direct nodes on the network (Fn 2.2)	Assured	90% of non-reporting units for which position and status reports is determined to be correct.
		Subjective determination that status determination of non-reporting units is accurate enough to be operationally useful (useful, marginal, not useful).
	Capable	100% of units can be tracked without their reporting.
	Timely	15 minutes required to determine non-reporting unit's characteristics.
		90% of non-reporting units for which a position is maintained within a given period of time.
		Average of 15 minutes within which a given non-reporting friendly location is updated.
5.8.3 Represent information visually, i.e., imagery, graphical, textual, tabular, schematic, geospatial or some other visible form (Fn 6.1)	Compatible	5% of required data elements missing in a representation, by visual representation type.
		Subjective determination of degree to which a visual representation meets the requirements of each user, by user (1-5 scale: 1 fully, 5 unmet).
		Standardisation of track zymology and associated data.
	Flexible	100% of information can be represented by visual modes or forms.
		100% of required visual representations can be simultaneously displayed.
		100% of required user defined specialized representations are available.

Uncontrolled copy when printed

	Usable	Maximum of two requests for clarification of a visual representation, by representation type. Maximum of two steps required to switch from one representation to another.
5.8.4 Integrate friendly, enemy, environmental and other information, Recognised Maritime, Air and Land Pictures (RMP, RAP, RLP) into a single representation, as desired (Fn 6.6)	Effective	Subjective determination of ease of understanding relationship between Red and Blue forces in the representation (1-5 scale: 1 easy, 5 difficult).
		Subjective determination of ability to predict red and Blue movements and their interactions with the representation (1-5 scale: 1 easy, 5 difficult).
	Flexible	More than one icon representation can be used to designate units.
		Force representations can be presented (user dependent): red only; blue only; red, blue, white; etc.
Usable	100% able to highlight individual units and drill down to their information with point and click.	
5.8.5 From a common set of available data, any node create and update a unique, user-defined representation of the situation as it applies to that node, including any plans, guidance, control measures, etc. as may apply (Fn 6.7)	Flexible	More than one mode or form of information can be incorporated into a single situational representation.
	Timely	8 seconds lag between real-world situation and situational representation.
		5 seconds between request and production of user representation.
	Usable	95% of user requested representations can be produced.
		Subjective determination of degree of completeness for the representation meeting their requirements (fully, partially, largely unmet).

Tier 1 JCA : Joint Interagency Integration

Tier 2 JCA : Interagency Cooperation Activities

Task : 8.1 Collect and Share Information (Op 2.2)

Sub-tasks	Attributes	Standards
8.1.1 Collect and transport sensor derived data (A2.3.3.1.4)	Extensive	95% connectivity with interagency nodes.
	Timely	8 seconds between product posting and availability for collaboration .

Task : 8.2 Provide Politico-military Support to Other Nations/Group/Government Agencies (Op 4.7)

Sub-tasks	Attributes	Standards
-----------	------------	-----------

Uncontrolled copy when printed

8.2.1 Conduct civil military operations in the area of operations (Op 4.7.2)	Compatible	90% of multi-national information sharing (MNIS) available.
	Effective	100% of MNIS operations supported and conducted.
	Timely	95% of information shared with multi-nationals in time to effectively conduct operations.
8.2.2 Provide support to DOD and other government agencies (Op 4.7.3)	Compatible	90% of multi-national information sharing (MNIS) available.
	Flexible	100% of multiple agencies supported, as needed.
	Manageable	95% quality support provided to multi-national forces to meet mission needs.
8.2.3 Coordinate politico-military support (Op 4.7.5)	Compatible	90% of multi-national information sharing (MNIS) available.
	Flexible	100% of multiple political-military forces supported, as needed.
	Manageable	95% quality support provided to multi-national forces to meet mission needs.

Task : 8.3 Coordinate and Integrate Joint/Multinational and Interagency Support (Op 5.7)

Sub-tasks	Attributes	Standards
8.3.1 Coordinate coalition support (Op 5.7.6)	Compatible	90% of multi-national information sharing (MNIS) available.
	Flexible	100% of multiple agencies supported, as needed.
	Manageable	95% quality support provided to multi-national forces to meet mission needs.
8.3.2 Incorporate non-DoD and Multinational elements into joint command and control processes (Fn 11.2)	Accessible	90% of non-DOD support requirements filled at time of execution.
		90% of required non-DOD elements have reviewed plans prior to publication.
	Flexible	95% of network nodes are available for non-DOD elements.
		95% integration of non-DOD doctrinal differences.
		95% coordination established with State Department, coalition partners and other non-DOD agencies.

Task : 8.4 Train Forces and Personnel (A3.2.4 and JFEO JIC)

Sub-tasks	Attributes	Standards
8.4.1 Modify organizational structure, to accept creation of established and expedient communities of interest's (Fn 14.3)	Capable	100% of new organizations introduced.
		6 hours required to establish a new organizational structure.
	Effective	Subjective determination of enhancement of operations with introduction of the new organization (improved, no change, degraded).

Uncontrolled copy when printed

	Flexible	100% of structures considered/tested.
--	-----------------	---------------------------------------

Tier 2 JCA : Information Management in Interagency Processes

Task : 8.5 Provide Public Affairs in the Area of Operations (Op 5.8)

Sub-tasks	Attributes	Standards
These attributes apply to task 8.5.	Accessible	More than one mode of access to media.
	Effective	90% of media output broadcast throughout the area of operations.
	Extensive	More than one type of media outlets available.

Task : 8.6 Publish Information on Environmental, Neutral, Unknown and Hostile Elements, Locations, Networks, Activities, Events, Sites, Platforms, Facilities and Individuals (Fn 3.3)

Sub-tasks	Attributes	Standards
These attributes apply to task 8.6.	Assured	100% of required horizontal and vertical geolocation accuracy reported in x, y, z coordinates. (NECC Standard)
		95% level of assuredness of location.
		95% of tracks with correct ids.
		95% of quality scores on quality/utility assessments fall within average.
	Sufficient	100,000 targets/day detected, classified, identified. (NECC Standard)
		95% of targets/day accurately located, classified/identified.
		95% of PIRs satisfied.
		5% of outstanding PIRs.
		90% of enemy offensive actions for which warning provided.
		95% of nodes receiving indications and warning.
		90% of time sensitive targets engaged successfully.
		10% of failure to respond to RFI.
	Timely	95% of PIRs requiring more than one collection source are satisfied.
		95% of RFIs are satisfied in a timely manner.
		95% timely collection, analysis and publishing of RFIs.
95% of manned reconnaissance missions requiring current intelligence have it before execution.		
		1 minute to convert in situ measurements into environmental profiles.

Uncontrolled copy when printed

Tier 2 JCA : Non-Governmental/ Private Volunteer Organization Integration		
Task : 8.7 Synchronize Execution Across All Domains (A5.2 and Op 5.7.4)		
Sub-tasks	Attributes	Standards
8.7.1 Communicate commander's intent and manage execution across a dynamic and diverse range of potential mission partners (Fn 11.3)	Extensive	100% of necessary nodes participate in managing execution.
		100% of required types of activity monitored by nodes.
		100% of reach-back nodes participate in execution management, as necessary.
	Flexible	100% of necessary nodes participate in managing execution.
		Commander's Intent can be delivered by more than one path.
	Effective	Collective execution management decisions improve execution (1-5 scale, 1 major improvement, 5 degradation).
	Timely	8 second latency of delivery of execution information (min).
		Subjective determination of whether execution management directions are delivered in time to modify execution (expedient, time late).

Table 7-A-1 Combined Requirements for COP

Uncontrolled copy when printed

CHAPTER 8

WEB SERVICES

INTRODUCTION

801. Web Services support Information Management (IM) principles articulated in Chapter 3 through the ability to manage and disseminate information to a large number of disparate users. Web Services also enhance systems interoperability by exposing authoritative data sources to external applications in an open and well-documented manner.

AIM

802. The aim of this Chapter is to provide guidance for the employment of web services in a low bandwidth maritime environment.

OVERVIEW

803. The key to Web Services is the availability of authoritative data and the ability to reuse it. While an IP network provides connectivity, it does not guarantee the ability to seamlessly share data. This is because IP-enabled applications often use application-specific mechanisms to format and transmit their data over networks. Web Services utilizes a 'web browser' to provide a common User Interface (UI) application between the data and the user. This negates the requirement for individual workstations to be loaded with numerous unique applications prior to being able to access and share information. Care must be taken to ensure that the browser being utilized on the network supports the required Web Service applications.

804. Intranets thrive on content currency and often contain large amounts of specialized information originating from wide and diverse sources. Content is more likely to be kept up-to-date when ownership is taken and there is positive management of content accuracy/relevance. This requires the establishment of bi-directional (heterogeneous) repositories and the adherence to IM procedures.

OBJECTIVE

805. The objective for web services is to create an '*electronic information library*' where:
- a. *information consumers* can easily discover, retrieve, and manage information based upon its characteristics advertised by information producers; and
 - b. *information producers* can advertise information availability and accessibility using metadata (information about data), data schema, and producer profiling mechanisms.

DEFINITIONS

806. The following terms are defined for use in this publication:

- a. Web-enabled – The presence of a front end user interface that is accessible through a web browser;
- b. Portal-enabled – A web-enabled application that feeds data through a portal device that controls the “look and feel” of the web page, instead of allowing the web server to interact directly with a client’s browser. The portal can connect to multiple web servers on behalf of the user and control the access, look and feel, and behavior for each web page all within prescribed “frames” that the user defines within their browser. (See para 814 (b) for more information.);
- c. Web Services – a system that uses standards and technologies to describe and deploy applications or services on a network in a consistent manner so that they can be discovered and invoked in a secure and reliable method;
- d. Search Engines – Computer programs that when queried for information (usually with a key word or phrase), find sites, web pages, and documents on the network fitting the description; and
- e. Service Oriented Architecture (SOA) - SOA is an emerging technological, procedural, and integration approach which is based on the concept of a service. It applies successful concepts and techniques proved by Object Oriented development, Component Based design, Enterprise Application Integration, and distributed computing. See Annex B to this chapter for more information.

FUNCTIONAL DESCRIPTION

807. Web Services are based on a Service Orientated Architecture (SOA) and can be described using the following three components:

- a. Service Requester – the mechanism through which a request to execute a Web Service is made;
- b. Discovery Agencies – the mechanism through which Web Service descriptions are published and made discoverable; and
- c. Service Provider – the component that processes a Web Service request.

808. Figure 8–1 shows these three components and their interaction. Interaction is possible because of the common middleware and the use of common communication standards and descriptions (Table 8-1 refers).

Standard	Description
Extensible Markup Language (XML)	A streamlined version of Standard Generalized Markup Language, developed by the International Organization for Standardization to define the structures of different types of electronic documents. XML can be used to store any kind of structured language and encapsulate data so it can be shared between otherwise incompatible computer systems.
Simple Object Access Protocol (SOAP)	Based on XML and Hypertext Transport Protocol. It provides a way for applications, including those running on different operating systems, to communicate and work together through remote procedure calls implemented via HTTP.
Universal Description, Discovery and Integration (UDDI)	Describes how to publish and discover information about Web services applications. It is a Web-based directory where someone can search for particular Web services and what they do.
Web Services Description Language (WSDL)	Based on XML, describes the kinds of software applications, or services, available on a particular network. Once someone develops a Web service, they can publish its description and link in a special UDDI repository. When someone wants to use the service, they request the WSDL file so they can determine its location, function calls and how to get to them. They use that information to construct a SOAP request to a server.

Table 8–1 Standards behind Web Services

809. When a service provider wants to make the service available to service consumers it is *published* using discovery agencies (UDDI registry). The service consumer who uses a client to access a service requester also uses this standard mechanism to *find* the service. The discovery agencies (UDDI registry) contain information in Web Services Description Language (WSDL) pertaining to the service and the access point for the service. The service consumer uses the WSDL description to construct a Simple Object Access Protocol (SOAP) message with which to *interact* with the service provider.

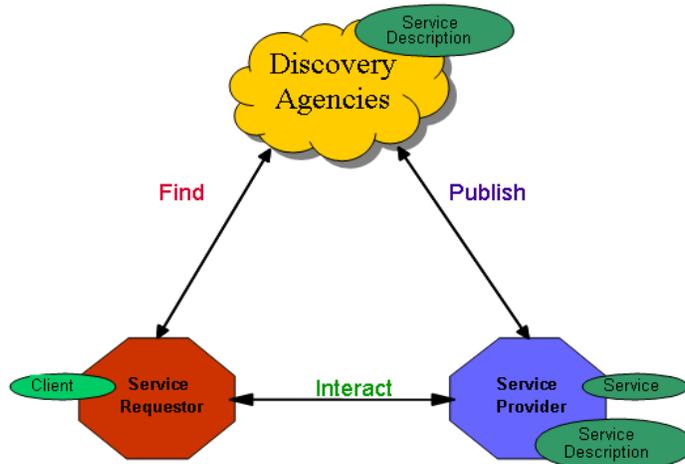


Figure 8–1 Service Orientated Architecture

WEB ADMINISTRATION**WEB ADMINISTRATOR**

810. The Web Administrator is responsible for the technical infrastructure of the web site(s). The administrator provides the tools to enable users to publish, access, and customize information. Tasks include registering users, maintaining functional stability and responding to web problems. Functional stability refers to the reliability of the site's interactive elements. This includes ensuring that hyper-links work properly.

WEB DEVELOPER

811. The Web Developer is responsible for developing / customizing web services.

INFORMATION MANAGER

812. The Information Manager oversees all content within a given functional area to ensure the timeliness, relevancy, and accuracy of information. At a minimum, the duties of the IM include enforcing maximum file size rules, monitoring user's adherence to formatting rules, and providing assistance.

INFORMATION PRODUCERS

813. Each functional area, as producers of information, determines what information they create and maintain on the web site. The information producer is responsible for keeping their portion of the web site and lower level sub-webs current and accurate.

PRINCIPLES

814. Web Services technologies and practices must:
- a. Support posting data to shared spaces in a timely fashion;
 - b. Support the parallel (i.e. Task, Post, Process, Use) vice serial (Task, Process, Exploit, Disseminate) processing of information. Example:
 - (1). Parallel: Units post their individual fuel state directly to the Task Group web site after each set of 'tank dips'. Result: CTG has the most up to date view of the overall state of fuel within the TG; and
 - (2). Serial: Units send record message traffic once per day, which includes fuel state at a given time. This information is collected by a member of CTG staff and then posted on the TG web site. Result: CTG has a time late view of the overall state of fuel within the TG once per day;
 - c. Enable Information Portability. Provide users with the capability to access the data they need, when they need it, from where ever they are;
 - d. Promote authoritative data and its reuse. Data that has been subsequently filtered or value-added should be posted back onto the network; and
 - e. Reduce the amount of email and supplant it in certain areas, such as attachment circulation.

REQUIREMENTS

815. The following requirements are mandatory:
- a. Information Awareness and Access – Users must know where and when information is available, and have the tools, procedures and capabilities to retrieve and analyze the required information. IM procedures in Chapter 3 (like the Information Dissemination Management Plan) and automated functions (like source registries) provide this capability; and
 - b. Information Repositories – The establishment of repositories and the identification and authorization of organizations / elements to create, compile, distribute, and dispose of data and metadata in these repositories.

CONNECTIVITY

PERSISTENT CONNECTIVITY

816. The lack of persistent connectivity coupled with the performance and latency characteristics of an MTWAN make accessing centralized applications impractical. The MTWAN environment requires applications that keep working productively at the local level in both the WAN connected and disconnected states. After all, a mobile platform loaded with 'immobile' applications (those that require persistent connectivity) is not mobile at all.

ONE-WAY REPLICATION

817. Traditional one-way data replication tools are suitable for updating a centralized database with information gathered in the field. This relegates mobile applications to being rudimentary information-display or capture devices, rather than true disconnected versions of the same enterprise applications.

BI-DIRECTIONAL REPLICATION

818. Alternatively bi-directional data replication solves many of the issues associated with distributed databases. By providing full read-write bi-directional replication capabilities, this technology makes it possible to deploy enterprise applications on mobile devices and to enable full access to application data, even in disconnected mode. In the background, there is a replication service that communicates any changes to data to all of the other databases. If a database is not online at the moment, it will be updated when it does come online. This, in effect, creates an application architecture where there can be thousands of dynamically linked databases, all communicating change to one another as needed. When implemented, this powerful capability provides "network transparency" to the user, since the application is free to roam between connected and disconnected modes without affecting user functionality (Annex A refers). Information ownership is critical when using a bi-directional replication service in order to enable the resolution of "replication conflicts" which may occur when two or more units modify or change the exact same information at the same time in a disconnected state.

TRANSACTION LOGGING

819. In order to ensure complete data integrity for updates and to perform incremental database backups, web replication products require some form of transaction logging capability. A transactional log provides a sequential record of every replication operation that has occurred during a given period of operation. This allows online server backup and recovery support. For example, if connectivity is lost, a transaction logging capability will enable replication to automatically recommence at the point it ceased, thus limiting duplication (non-transaction logging replication services would have to start from the beginning) and consequently duplicate use of expensive and often limited communication bandwidth.

WEB CONTENT / PAGES

HOW USERS EXPERIENCE THE WEB

820. Readers experience web pages in two ways:
- a. As a direct medium where pages are *read online*; and
 - b. As a delivery medium to access information that is *downloaded* for use in applications or printed onto paper.

821. How readers use the information should govern the type of document posted. Documents to be read online should be concise, with an appreciation of the available bandwidth available. Documents that will most likely be printed and read offline should appear easily on a page.

USERS CHOICES

822. Users tend to choose the first reasonable option presented to them vice the best option. This is a reflection that the users are usually in a hurry, and the cost for guessing wrong is only an additional click or two. Also in the case of poorly designed sites, weighing the options might not improve the user chances.

RESPONSE TIMES

823. The basic advice regarding response times has been consistent for almost thirty years:
- a. 0.1 second is about the limit for having the user feel that the system is reacting instantaneously, meaning that no special feedback is necessary except to display the result;
 - b. 1.0 second is about the limit for the user's flow of thought to stay uninterrupted, even though the user will notice the delay. Normally, no special feedback is necessary during delays of more than 0.1 but less than 1.0 second, but the user does lose the feeling of operating directly on the data; and
 - c. 10 seconds is about the limit for keeping the user's attention focused on the dialogue. For longer delays, users will want to perform other tasks while waiting for the computer to finish, so they should be given feedback indicating when the computer expects to be done. Feedback during the delay is especially important if the response time is likely to be highly variable, since users will then not know what to expect.

WEB PAGE GUIDELINES

824. Web pages that are concise and easily reviewed reduce the user's cognitive load, which results in faster, more efficient processing of information.

SHORT TEXTS

825. Reading from computer screens is slower than reading from paper as concise text contains less information to process.

REVIEWING TEXT

826. The following suggestions can improve the quick review of text:

- a. Highlighted keywords (hypertext links serve as one form of highlighting; typeface variations and color are others);
- b. Choose meaningful sub-headings;
- c. Employ bulleted lists;
- d. Use one idea per paragraph (users will skip over any additional ideas if they are not caught by the first few words in the paragraph). Where appropriate use the inverted pyramid style, starting with the conclusion;
- e. Half the word count (or less) than conventional writing; and
- f. Use uppercase letters sparingly. Uppercase words are not easy to read as mixed case words, and can make a page look busy and loud.

POSTING DOCUMENTS

827. All documents posted should have:

- a. An informative title (which also becomes the text of any bookmark to the page);
- b. The creator's identity (author or institution);
- c. A creation or revision date;
- d. At least one link to a local home page or menu page*; and
- e. The "home page" URL on the major menu pages in your site*.

Note: An asterisk (*) denotes a feature that can be provided automatically by a template.

HIERARCHY OF INFORMATION

828. Careful thought should be placed as to the posting location of documents to establish an efficient hierarchy for the information. This will allow users to get information in the fewest possible steps.

WEB INTERFACES

829. A good Web Interface will provide ease of use for even novice users. For the web developer, it is relatively easy to construct and provides rich and expanding support for a variety of GUI components and processing models. Other rich media capabilities such as Xforms and Flash also allow developers a wide range of choices over what elements can be used to develop Web interfaces. Care must be taken to the impact on bandwidth which may be caused by the interface element selected.

PORTAL

830. An information portal is a concept that serves as a single gateway to an organization's information and knowledge base. An information portal can comprise the following elements:

- a. Access / Search – Allows a user to get all the information needed (but no more) in the desired context;
- b. Categorization – A portal can categorize all information so that it is delivered to the user in context needed;
- c. Collaboration – Allow individuals to collaborate regardless of geographic location;
- d. Personalization – The information provided to the individual is personalized to that person's role, preferences and habits.

TEMPLATES

831. Templates provide tailored views of documents from within a web browser. Templates provide the following advantages:

- a. They bring consistency and predictability to web pages across the MTWAN;
- b. Operators at each site become information/content managers with the responsibility of populating and managing each local site with documents, briefs and other pertinent information rather than on the mechanics of developing web pages; and

- c. They provide easy navigation within the site. (Users become familiar with the layout of the site and can return easily to the home page and to other major navigation points in the site.)

CONCLUSION

832. Web Services are an important and evolving technology that can be used to support the war fighter's information requirements. It can be employed to improve interoperability, information management, and collaboration.

WEB-ENABLED DATABASE REPLICATION

INTRODUCTION

1. Bi-directional data replication of web-enabled databases solves many of the issues associated with distributed databases. By providing full read-write bi-directional replication capabilities, it is possible to deploy enterprise applications on mobile platforms and to enable full access to application data, even in a disconnected mode.

AIM

2. The aim of this annex is to describe and provide guidance for bi-directional web-enabled database replication in a low bandwidth environment.

OVERVIEW

3. By providing full read-write bi-directional replication capabilities, it is possible to deploy enterprise applications on mobile platforms and to enable full access to application data, even in disconnected mode. With a common web-enabled database at each location, operators are able to browse the site on their local LAN (or work station) without having to browse off-ship in order to reach needed information on a remote server. Local browsing provides two advantages; it provides a high speed ‘surfing’ experience – providing faster access to required information in both connected and disconnected state, and it reduces the bandwidth requirement/utilization for external communications since information is transferred only once to the unit – even though it can be accessed multiple times. Any changes made locally to the database in an offline state will automatically be replicated to the network upon reconnection.

4. The template-centric database allows operators at each site to become information/content managers with the responsibility of populating and managing each local site with documents, briefs and other pertinent information rather than on the mechanics of developing web pages.

REPLICATION ARCHITECTURE

5. There are three basic types of replication architectures:

- a. Hub-Spoke;
- b. Meshed; and
- c. Federated Hub-spoke.

HUB SPOKE

6. A hub-spoke replication topology has proven to be an efficient method for replication. Figure 8–A–1 illustrates typical hub-spoke architecture with the vast majority of nodes having one or possibly two links, juxtaposed with a tiny number of nodes that have a large number of connections.

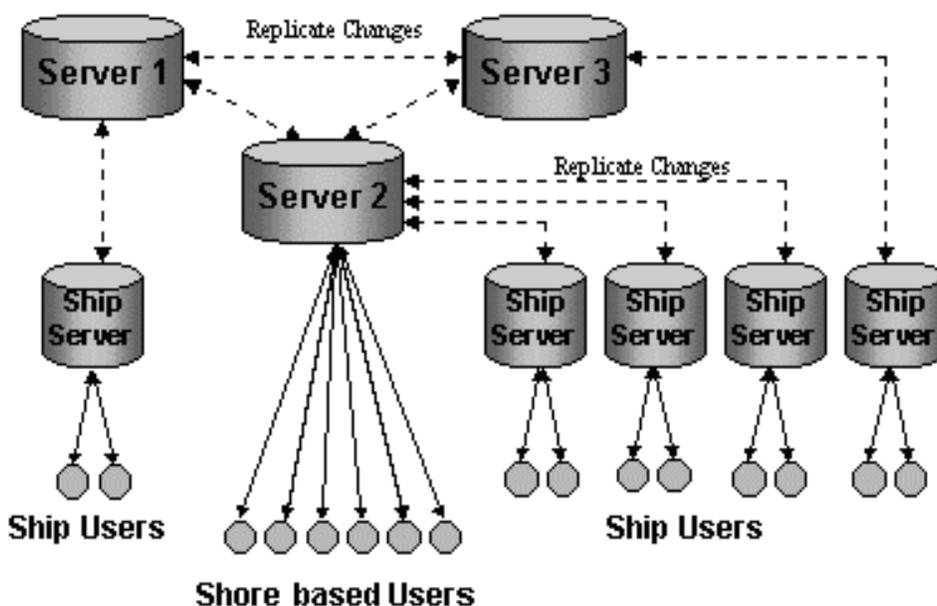


Figure 8–A–1 Generic Replication Architecture

7. The architecture minimizes bandwidth consumption by replicating only changes in data between remote web servers and master servers. Replication to the master servers can be scheduled to occur on any periodic basis, as dictated by the overall operational needs of the TF/TG Commander. External (off ship) connectivity is required only for replication of web site databases. This minimizes the requirements for connectivity and increases operational capability and effectiveness. It also provides a means for continuing operations during short periods of EMCON silence.

MESHED ARCHITECTURE

8. Figure 8–A–2 illustrates a ‘meshed’ replication architecture. In a meshed model, multiple replication connections are established with all units within the network. This provides a highly flexible and survivable information-sharing model. The meshed model allows for information sharing between TG units using a fully dynamic LOS tactical IP sharing network with no shore connectivity. It must be noted that a meshed architecture can increase the bandwidth requirement due to the multiple server-to-server connections. Therefore only key tactical information databases should be shared in a low bandwidth LOS tactical IP sharing environment. Remaining, non-critical databases should follow Hub-Spoke architecture for delivery to mobile units.

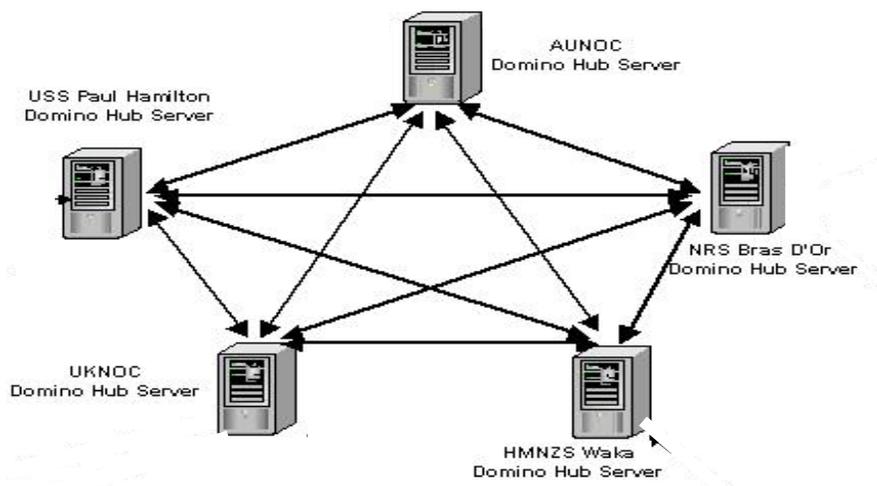


Figure 8–A–2 Mesh Replication Architecture

FEDERATED HUB SPOKE

9. Figure 8–A–3 illustrates a hub-spoke architecture with multiple hubs vice an architecture employing a single hub. This is a combination of a hub-spoke and meshed architecture in order to combine survivability with bandwidth reduction. Rather than a hierarchical model, a federated hub system is preferred when multiple hubs are employed with large bandwidth availability.

SCALABILITY

10. These topologies are scalable in that additional servers can be added without adverse effects.

SURVIVABILITY

11. Scalable topologies are quite survivable against random failure, but are highly vulnerable to a focused attack because of the critical role of the hubs in the network. Research has shown that up to 80 percent of the nodes in a federated hub-spoke network can be randomly removed without compromising the functionality of the networked whole. However, a coordinated attack that disables 5 percent to 15 percent of the hubs simultaneously would compromise the system.

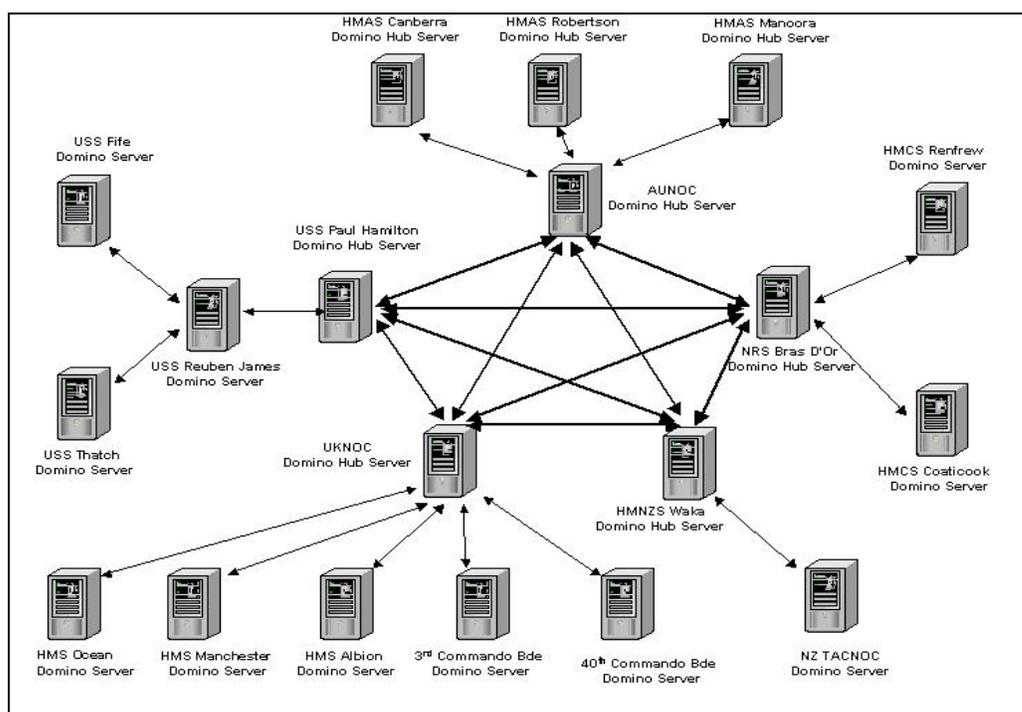


Figure 8–A–3 Federated Hub-Spoke Replication Architecture

REPLICATION PROCESS

12. In general, web enabled databases are composed of unstructured document objects such as ASCII text fields, Rich Text Format (RTF) fields, graphics, file attachments of different types, or any combination of the above vice a traditional relational database. Subsequently, documents and files of any type can be added to such web sites.

13. During each replication cycle, the servers compare their document databases with those of the hub server and vice versa. The differences in the data fields (or the delta) is noted and then exchanged between the servers. At the end of the replication cycle, all servers at all sites contain an identical set of documents. This significantly reduces the bandwidth required.

14. The use of ASCII Text and RTF fields provide the most efficient means of replication, as text fields are compared and only the differences in text are sent. File attachments are treated as one data field, any change to an attached file require the whole file to be retransmitted. This means that a 50KB Word document that is 'attached' to the web site for posting vice using 'cut and paste' into a RTF Field would result in approximately the same data transfer size on initial replication. Any subsequent changes to that information, even a change as small as adding a single letter to a word contained within the document, would result in the entire Word document being retransmitted for the file attachment (50KB); however, only the single character letter would be transmitted for the change in the RTF Field – a few bytes.

TRANSACTION LOGGING

15. The role of transaction logging is to keep track of the replication status. If communications (or connectivity) are lost for any reason, replication will cease. However, when communication is re-established, replication will automatically recommence at the point it ceased, thus limiting duplication and consequently (often) expensive communication and satellite time.

REPLICATION CYCLE / TIME

16. Users should be cognizant that a number of replication cycles are often required to transfer documents from one unit to all participants. The accumulated replication time will be dependent on the network architecture and available bandwidth. Replication should be set to occur IAW the OPTASK IM and OPTASK NET.

FORCED REPLICATION

17. If necessary, the replication process can be initiated manually, or 'forced', in order to speed information dissemination vice waiting for the scheduled replication cycle.

STREAMING REPLICATION

18. This method involves a single server request that performs a PULL of all the data into the database. This is an improvement over the non-streaming method of requesting and acknowledging one database document or note at a time. Streaming replication means that you do not need to wait until the replication completes before you see replicated documents in folders. They appear individually as soon as they are pulled into the system and you can begin to work on them before the database finishes replicating. Benefits include faster replication, partial replication and potentially less network traffic due to a single streamed Remote Procedure Call (RPC), and a reduction of Acknowledgement (ACK) TCP/IP responses.

NETWORK COMPRESSION

19. Network compression (if available) should be employed to reduce transaction times, and employ bandwidth efficiently. When enabled, data is automatically compressed (ideally it requires no user intervention) before it is sent over the network. The degree of compression will be dependent on the file type and the compression technology.

TYPICAL REPLICATION WEB PAGE

INTRODUCTION

1. The best-designed replication sites allow readers to enter the site, find what they want, and easily print or download what they find. Non-essential graphics should be minimal and non-distracting. Additionally, content and menu structure must be carefully organized to support fast search and retrieval, easy downloading of files, and convenient printing options. Contact time is typically brief in replication sites: the shorter the better.

AIM

2. This Appendix describes a typical bi-directional heterogeneous replication page, which is used to disseminate information within a TF/TG.

OVERVIEW

3. Templates provide narrative and design consistency for the site. They also facilitate site maintenance.

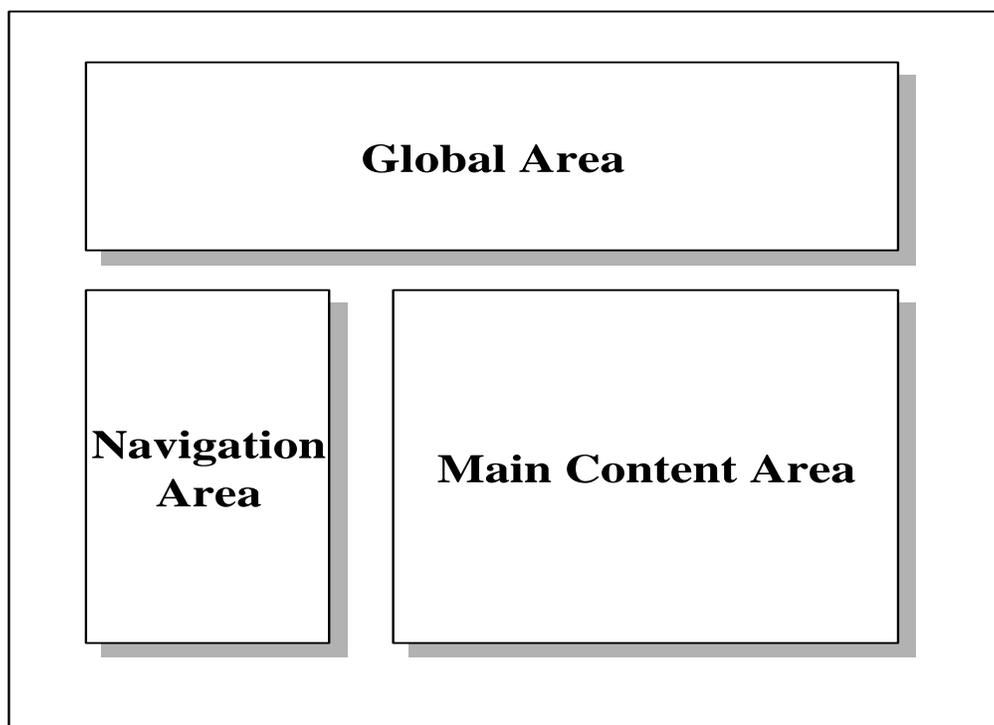


Figure 8-B-1 Typical Page Structure

PAGE-LEVEL STRUCTURES

4. The general navigation and layout conventions for a typical TF/TG replication template follow major website conventions. Most users will be familiar with these conventions.
5. Page-level structures include the distribution of content, applications, and navigation tools. Many pages use the basic three-panel structure shown in Figure 8–B–1. The top area contains global information about the site, the left side area contains navigation controls and links to commonly used objects, and the large central panel is home to the substantive content of the portal.

GLOBAL AREA

6. The global area is consistent across the web site and often provides links to a home page, contact information, accessories, or other frequently used applications. In some cases, the area is used to present monitoring information such as the status of threat levels. Figure 8–B–2 highlights the common elements.

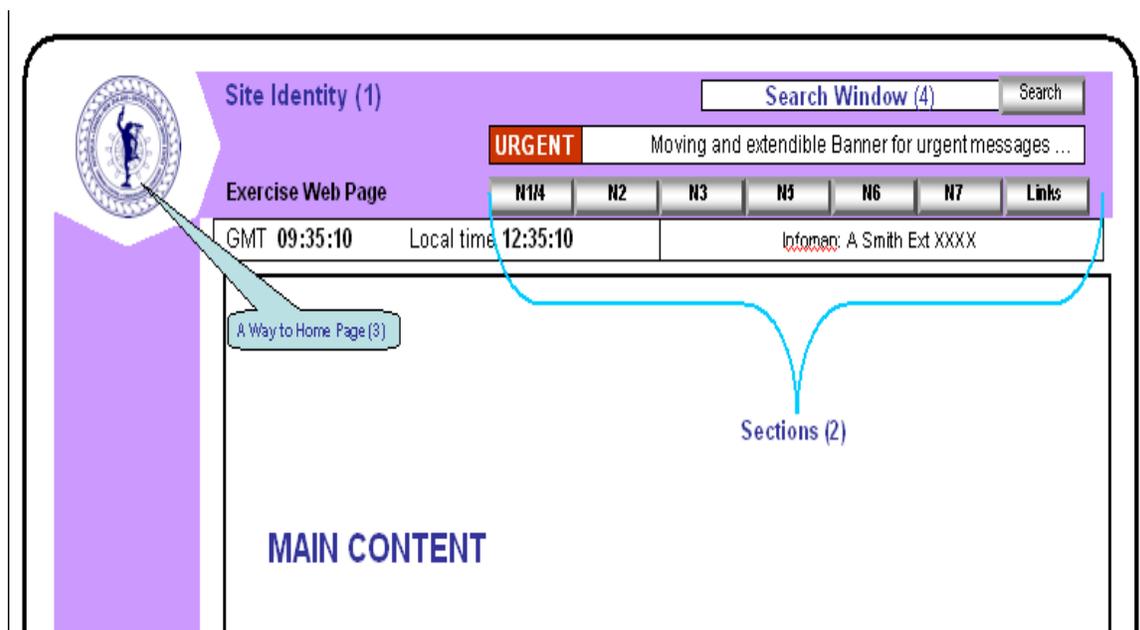


Figure 8-B–2 Global Area Content

7. The Site Identity or logo provides users with a reference to what site they are in. Sections provide the links to the main sections of the site (i.e. the top level of the site)

hierarchy). In the case of most TF/TG sites, this is the links to information grouped along traditional military functional lines, referred to as the Continental Staff System.

Uncontrolled copy when printed

NAVIGATION AREA

8. The navigation rail provides a localized context for users. This provides an immediately visible and easily accessible path to related components in the site, while keeping the user from being overwhelmed by the full breadth of the site.

MAIN CONTENT AREA

9. The main window is the target area for viewing navigation results such as libraries, reports, and documents.

FOOTER NAVIGATION

10. A common design convention is to feature certain options at the end of the page, such as appropriate time zones etc.

MARITIME TACTICAL SERVICE ORIENTED ARCHITECTURE (MTSOA)

INTRODUCTION

1. Service Oriented Architecture (SOA) is an emerging technological, procedural, and integration approach which is based on the concept of a service. It applies successful concepts and techniques proven by Object Oriented software development, Component Based design, Enterprise Application Integration, and distributed computing.

AIM

2. This chapter describes current SOA design and implementation considerations in support of a MTWAN.

DEFINITION

3. Maritime Tactical Service Oriented Architecture (MTSOA) is a distributed system of independent services that permit the user to discover, interact with, and use information, and make it available at the tactical edge. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with pre-defined conditions and expectations.

4. The key factors are:

- a. MTSOA is built on the standards of the World Wide Web leading to cost-effective implementations on a global basis;
- b. Services are “loosely-coupled” allowing for much more flexibility than older technologies with respect to re-using and re-combining the services to create new functions and capabilities;
- c. MTSOA requires data to be pushed forward to the tactical edge in a distributed architecture as much as possible, rather than being stored central repositories;
- d. MTSOA best practices create designs which embody processes and governance, and enhance the ability to outsource and extend processes to coalition partners;
- e. MTSOA encompasses legacy (i.e. existing) systems and processes so that the usefulness of existing investments can be preserved and even increased.

OVERVIEW

5. Over the years, many system users have found that inherent processes within Enterprise Resource Planning (ERP) systems are too restrictive to accommodate necessary operational functions. If these processes could not be changed, generally, a modification to the ERP software was the result. The advent of SOA software design promises a more flexible and adaptive application architecture. The foundation of this approach is standardization of software design and development based upon industry web services interoperability standards. SOA does not replace ERP systems but provides the ability to “loosely couple” services (business functions) as opposed to the “tightly coupled” ERP approach.

6. Service-Oriented Architecture is a maturing technology that directly supports the war fighter vision of enterprise-level processes and services that optimize investment and build enhanced capability. SOA can be views as a software design approach in which a client application requests one or more services from another application that provides similar or complementary services. The design allows internal and external processes to be combined and recombined to support flexibility in process execution.

7. A **service** - in the context of SOA - is a function or process that is well-defined, self-contained, and doesn't depend on the context or state of other services. Overall, SOA is a collection of services that communicate via a high-level abstraction layer, using existing and emerging Web Services standards.

8. Taking a SOA approach would plan to provide or obtain a service over the WAN using these Web Services standards. The term “services” in the context of web services refer to the technical standards that allow communication between the collection of **services** in a service-oriented architecture, which in turn combine to enable an end-to-end process and operation. Standards are integral to web services, and web services are key to a Service-Oriented Architecture.

9. The technical components of a **service** as used in SOA consist of a service interface and a service implementation component:

- a. The interface component creates interoperability between services; and
- b. The implementation component produces a differing result based on the reuse of the individual components.

10. Once defined, services can be used and reused, combined and recombined by multiple different “consumers” of the service. The use of common technical web services standards as the foundation of the software application supports flexibility in business process execution. This loosely coupled structure provides business process flexibility that more tightly integrated software applications have not delivered.

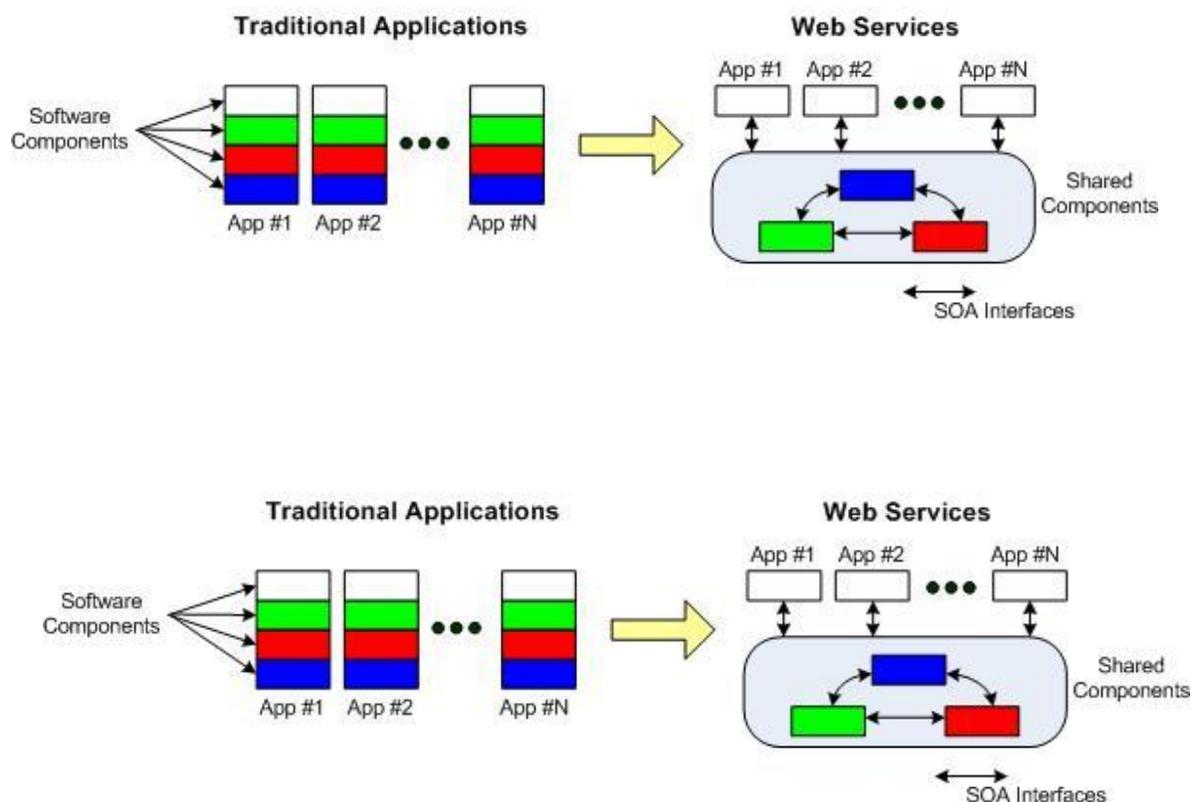


Figure 8-C-1: Software Building Block Reuse

BENEFITS OF SOA

11. If software applications are built using SOA standards and principles, war fighting processes rendered as services can be combined to create a holistic solution – combining multiple traditional elements in new ways to augment current capabilities or implement new capabilities.

12. A Service-Oriented Architecture if implemented properly:
- a. Enables change and transformation by providing visibility to operational processes from the Tactical to the Strategic;
 - b. Forces technology leadership to think in terms of operational and war fighting processes;
 - c. Minimizes the impact of changes to software code on other software components through “loose coupling”;
 - d. Enables propagation of consistent, organization-specific processes;
 - e. Helps realize a greater return of investment;
 - f. Increases redundancy of the systems;
 - g. Eases future interoperability internally and to external third parties; and
 - h. Data is pushed from centralized information stores to disparate locations throughout the network;

SOA IMPACT ON A MTWAN

13. SOA governs how internal and external services interact on the MTWAN. As new services are introduced, or more users invoke such services, an increase in network communication will occur. This communication can be simple data passing or complex coordination amongst many service components. As these services proliferate within the MTWAN, the following network effects will be experienced:

- a. Site-to-site traffic volume will grow – potentially exponentially. Since new applications and capabilities will be created using both new and reused code, the code execution will be distributed throughout the MTWAN. As services become a collection of services, all with increased network traffic requirements, the bandwidth utilized will increase. Additionally, current protocols which facilitate SOA principles such as XML are verbose and not optimized for low bandwidth environments;
- b. Low latency will be an increasing critical network characteristic for user performance. Applications based on Web services depend more on machine-to-machine communications, and machine-to-machine interactions are always the most time-sensitive traffic on networks. Applications today mostly execute on a single computer; interprocess communications are handled by the computer system bus. When processing is distributed with Web services and SOA, interprocess communications are carried over the network. That's a lot of time-

sensitive traffic now traveling over the MTWAN. With SOA, network performance will directly affect the end user's experience;

- c. Less predictable traffic patterns. Web services can be combined in often unpredictable and complex ways. The possible combinations are endless. Network flexibility will be an increasingly important characteristic in order to have successful SOA applications however overall network management will become more complex;
- d. Quality of Service (QoS) is implemented to insure timely delivery of delay-sensitive traffic. QoS only works if the network can easily identify high-priority packets. There is only one way that QoS could work with a proliferation of SOA-based applications: deep packet inspection, which has significant performance, cost, security, and application transparency issues. It will be nearly impossible to ascertain when a particular service is being used as part of a mission-critical application or not. Network administrators will require understand the functional details of all applications on the MTWAN or else the risk exists that appropriate QoS is not implemented correctly;
- e. Security architectures and suites will become more complex since software components will be dynamically exchanging information throughout the MTWAN; and
- f. More sensitivity to network downtime. As mission critical or essential SOA-based applications are deployed, they will require a high-availability network infrastructure that is proven in a tactical environment with very minimal downtime. High-availability network infrastructures are extremely difficult and costly over high latency satellite MTWANs.

CONCLUSION

14. SOA can be regarded as a style of Information System architecture that enables the creation of applications that are built by combining loosely coupled and interoperable services. These services interoperate based on a formal definition which is independent of the underlying platform and programming language. The interface definition hides the implementation of the language-specific service. SOA-compliant systems can therefore be independent of development technologies and platform. Additionally, applications running on either platform can consume services running on the other as Web services, which facilitates reuse across the MTWAN.

15. SOA can support integration and consolidation activities within complex network systems, but it does not specify or provide a methodology or framework for documenting capabilities or services. Benefits can be leveraged with this approach however there will be significant impacts to the MTWAN. Increased network communication traffic coupled with complex networking challenges such as more delay sensitivity, less predictable traffic pattern,

and QoS and security re-engineering are a number of the difficulties which will be encountered.

Uncontrolled copy when printed

CHAPTER 9

DISTRIBUTED COLLABORATIVE PLANNING

INTRODUCTION

901. Military forces rely upon shared information from multiple sources, including intelligence, thoughts, plans, and ideas. This information is used to plan, deploy and execute operations. The act of sharing this information to develop plans collectively is called collaboration. As such, information sharing and collaboration are essential aspects to war fighting.

902. Until recently, collaboration between dispersed units has been confined to formatted messages and voice circuits. This has limited both the scope of information that could be conveyed and the format in which information could be presented. Lengthy messages were often required to convey the Commander's plan and good comprehension skills were required to assimilate details and understand the intent in other units. This system was formalized and best implemented by a 'top down' planning approach. In such an environment, collaboration was limited.

903. Today, real-time technologies, such as instant messaging chat, audio conferencing, shared whiteboards, screen sharing, and application sharing provide a new, rich dimension to collaboration. Planning can effectively reach all members who need to be involved despite their geographic location. Information can be presented in a wider range of media formats. 'Bottom up' planning and informal or offline planning provide alternative means of collaboration vice the traditional 'top down' and formal approaches.

904. Real-time technologies have:

- a. Enhanced the relevancy of information;
- b. Improved assimilation of information by the warfighter;
- c. Promoted information sharing and the generation of new ideas; and
- d. Increased the level of situational awareness and understanding.

905. Furthermore, recent experiences have highlighted the effectiveness of employing these synchronous collaboration tools in combination with the asynchronous collaborative infrastructures such as email and Web Services.

AIM

906. This chapter provides guidance for the employment of Distributed Collaborative Planning (DCP) within a maritime military environment.

OVERVIEW

IMPORTANCE

907. Critical to gaining and sustaining the initiative in warfare is the ability to stay inside the enemy's planning-cycle time. This requires real-time collaborative tools to store, share, and distribute information and knowledge to war fighters that may be geographically dispersed.

TIMELINESS

908. Real-time capabilities provide many benefits to maritime communication and collaboration. These include:

- a. Faster, better decision making, reducing the decision cycle;
- b. Additional methods of expression to communicate meaning, helping to make communication rich and complete;
- c. Improved communication with the Task Group members; and
- d. Closer ties among the diverse Task Group members in a Coalition environment.

EFFECTIVENESS

909. It is the combination of the awareness; conversation, and shared objects features that provide the war fighter with a powerful collaborative tool. Together they make collaboration as convenient and as effective as face-to-face conversations.

COLLABORATIVE PLANNING SPECTRUM

910. Figure 9-1 and Table 9-1 illustrate the broad spectrum of planning that can be conducted using DCP. Generically, the spectrum can be delineated by time and to the degree the session is planned. This concept therefore enables DCP tools to be tailored for each type of meeting with a subsequent set of protocols being standardized for each session

	DELIBERATE	ADHOC	NOTES
UNCONSTRAINED	Daily Briefing	Fireside Chat	1. Documents provided in advance 2. Replication able to take place 3. Bandwidth Efficient 4. Higher level tools such as VTC can be utilized
CONSTRAINED	Contingent Operations	MEDIVAC, SAR, Crisis THREAT WARNING RED	1. No time to replicate in advance. 2. Extensive use of Whiteboarding 3. Bandwidth intense 4. VTC not supportable due to extensive use of lower bandwidth tools
NOTES	Planned Follows a set format Standard Topics	Unplanned, No Format	

Table 9-1 DCP Spectrum

AWARENESS

911. Awareness makes real-time network conversations as convenient as deciding to talk to someone simply because one is aware of their presence. Effective real-time collaboration relies on the same ad hoc feeling as a hallway encounter, instead of making users go through cumbersome efforts to set up a simple meeting or a conference call. This facilitates the dissemination of information and improves situational awareness.

CONVERSATION

912. Critical to successful collaboration is the capability to select from a suite of tools to maximize efficiency and minimize any loss of information. Operators should have the ability to select from a suite of real-time conversation tools: instant messages, text chat, audio, and video. For quick clarification, chat may be appropriate. Voice or video may be more efficient for longer or more detailed conversations. Other interaction may require the precision of the written word so that the accurate and complete meaning is captured and agreed upon.

SHARED OBJECTS

913. Collaboration between people predominantly involves conversation. Frequently, these conversations refer to some sort of object: a message, a presentation or the deployment of forces. When some or all of the participants have shared access to that object, the conversation — the collaboration — is richer and more complete.

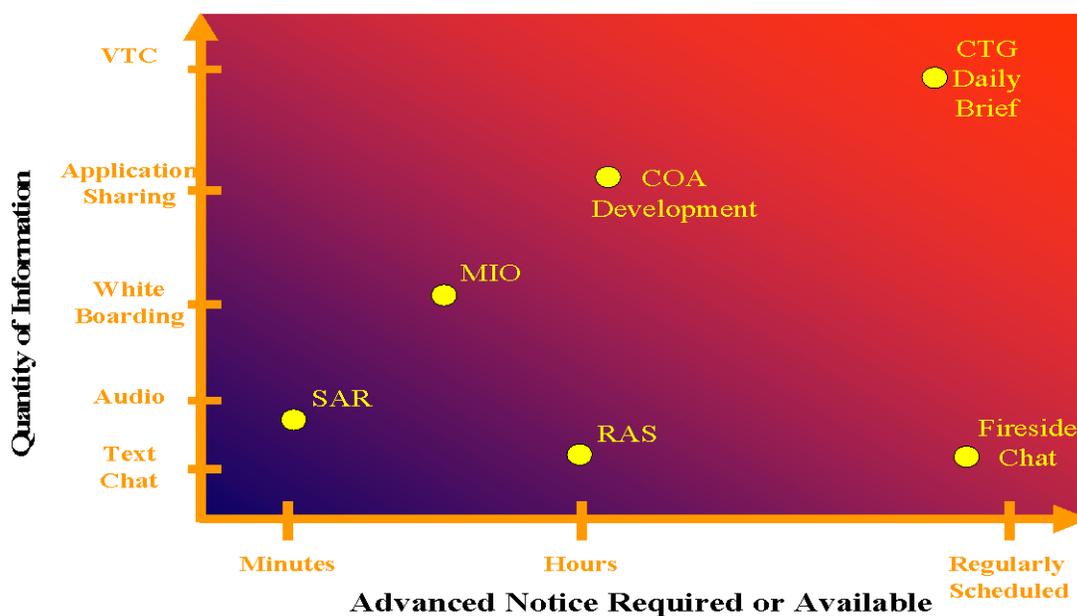


Figure 9-2 Collaborative Planning Spectrum

GLOBAL ADDRESS BOOK

914. The need for an integrated Global Address Book cannot be overemphasized. This Global Address Book:

- a. Provides Awareness of who is on-line and available to collaborate synchronously;
- b. Authenticates users in establishing DCP sessions; and
- c. Authenticates users in the access and posting of web documents.

BLENDING ASYNCHRONOUS AND REAL-TIME COLLABORATION

915. The impact of real-time collaboration is maximized when it is combined with traditional or asynchronous collaboration. Together, they make computer-based collaboration a more natural way to work. This blend is critical, since users naturally move from one mode of interaction and work to another, usually without giving the matter much thought. The value

of these technologies is enhanced when they are integrated in a way that mirrors MTWAN business practices. From real-time awareness, an operator can determine that a colleague is available to talk. In a blended real-time and asynchronous environment, the user could open a database and look up the name of the person the operator wants to meet with. If that person is currently online, the user can engage them in an online meeting immediately; if not, the user could send them an email to schedule an online meeting later. Instead of replying to an Email, a user could start a conversation with one or many Email recipients. After editing a document as a shared object, a user could save the revised document in any number of places, such as in discussion databases, bulletin boards, or internal Web sites, for review by others. An informative online meeting, such as the Commanders Intent, could be archived. Colleagues who missed the meeting could replay both the conversation and the shared objects.

916. Figure 9–2 highlights the possibilities in terms of synchronous and asynchronous collaborative tools with respect to the location of participants.

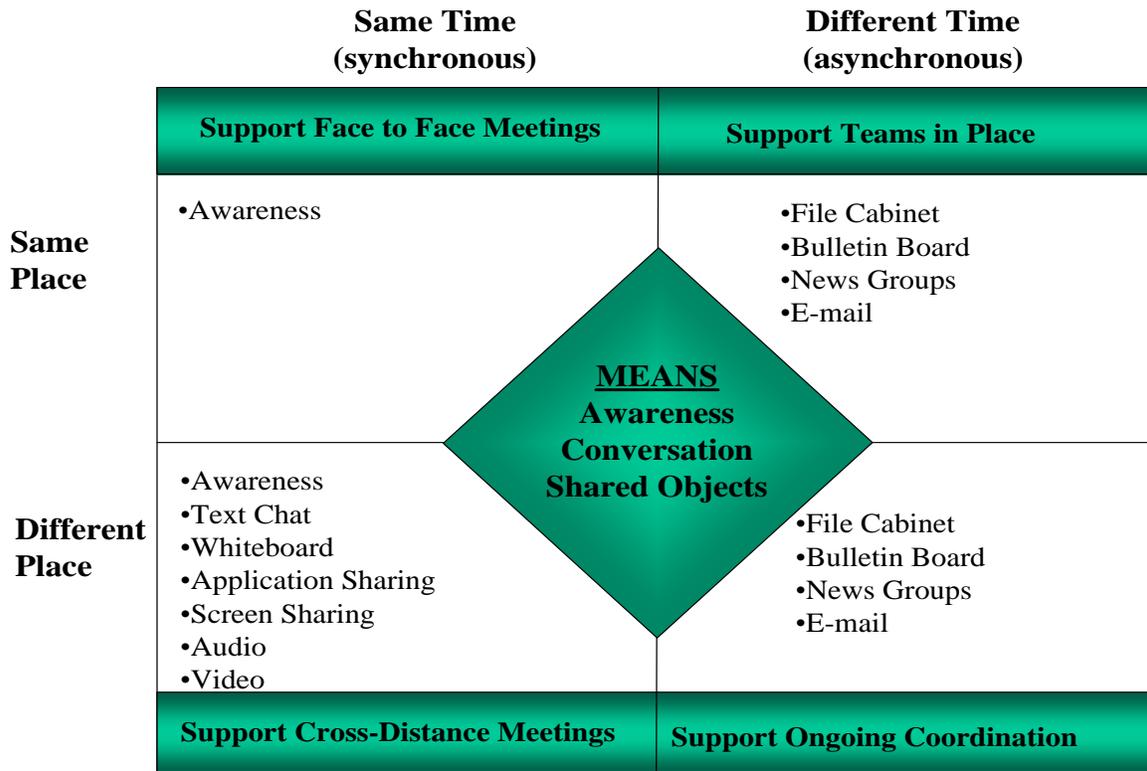
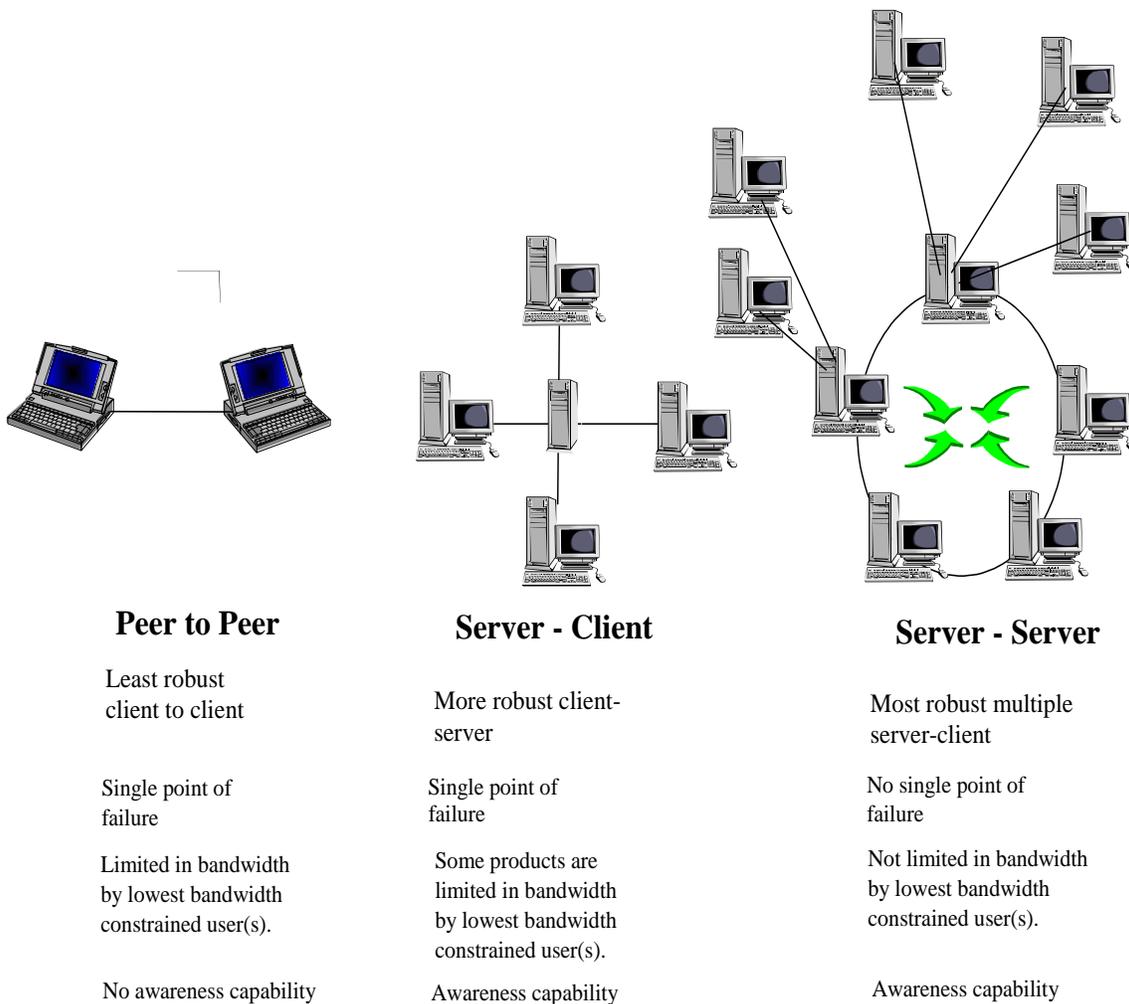


Figure 9–2 DCP Characteristics

Uncontrolled copy when printed

CONFIGURATION

917. Generically, there are three DCP configurations: peer to peer, server – client, server – server. These are represented in Figure 9–3, along with their characteristics. Peer-peer configurations are a low cost solution for engineering temporary interoperability between a low number of users when a server is not available. Server-client configurations can support greater number of users and is more robust. In a hub-spoke environment servers could be connected, sharing the Global Address Book, and allow users to Collaborate across multiple servers. The server-server solution avoids a single point of failure and provides some load-sharing capability.



Uncontrolled copy when printed

Figure 9–3 DCP Configurations

BANDWIDTH LIMITATIONS

918. The configurations in Figure 9–3 assume efficient connectivity and high data rates. In the low bandwidth maritime environment these conditions will seldom exist in almost every circumstance, efficiency of the Network, whatever its configuration, will be determined by the data rate achievable by the communications bearer. It is therefore important that information management practices be implemented within all DCP sessions to ensure that information quantity and detail does not overload the network and prevent its subsequent use in a timely and effective manner.

919. Scalability, whether inherent in the tool or achieved through the selection of tool(s), combined with effective standard operating procedures are required to support DCP in a low bandwidth environment.

TOOLS

920. Efficient, flexible, instantaneous communication is critical for successful Service, Joint, Combined and Coalition Operations. DCP tools must meet these objectives as well as being intuitive and easy to use. The selected DCP suite would normally comprise the tools detailed in Annex A 9A03 sub paragraph b.

REQUIREMENTS

921. In a coalition environment, DCP requires tools that:

922. Are capable of providing reliable and scalable services within the constraints of the tactical communications environment;

- a. Support both deliberate and adhoc planning;
- b. Support the tool sets and functions listed in Annex A; and
- c. Conform to the developing standards listed in Annex B.

CONCLUSION

923. The adoption of DCP tools and processes are critical to improving the effectiveness and speed of the commander's planning and operational decision-making process. This chapter outlines the scope, applicability and requirements of DCP. It is for the commander to make the maximum use of this capability by clear direction in their operational intentions.

DCP STANDARDS

INTRODUCTION

1. The early adoption and implementation of agreed-upon standards was the key to widespread implementation and industry-wide innovation in networks. The success of real-time collaboration will be no exception. In each of the critical elements of real-time collaboration – awareness, conversation, and shared objects – there are varying degrees of standards development and industry acceptance. The chief benefit of standards, of course, is the promise of interoperability among products, applications, and tools from a variety of vendors. Furthermore, as standards are adopted and mature, they raise the level of functionality and ease-of-use across the entire spectrum of applications that are developed in accordance with those standards. While the integration of awareness, conversation, and shared objects is critical to real-time collaboration, each element has unique characteristics that justify different protocols for each one.

STANDARDS

AWARENESS

INSTANT MESSAGING AND PRESENCE PROTOCOL (IMPP)

2. Today there is no generally accepted standard for the exchange of awareness or presence information. Awareness is a low-overhead activity — the interactions are usually short in duration and there is little bandwidth required. Currently, several companies have proprietary protocols for exchanging awareness information. Lotus, Microsoft, and others are joined in an IETF effort to produce a single protocol. This working group is called IMPP (Instant Messaging and Presence Protocol).

CONVERSATION

H.323

3. The requirements of conversation protocols differ greatly from awareness. Conversations can be text, audio, or video, and therefore require varying levels of bandwidth. For audio and video communications, the main protocol is H.323. The H.323 specification was ratified by the International Telecommunications Union (ITU). H.323 provides a foundation for audio and video communications across IP-based networks, including the Internet. Additional key benefits include:

- a. Interoperability. H.323 establishes standards for compression and decompression of audio and video data streams, allowing equipment from different vendors to communicate. H.323 also sets methods for clients to communicate capabilities to each other;
- b. Platform and application independence. H.323 is not tied to any hardware or operating system;
- c. Bandwidth management. Video and audio traffic is bandwidth-intensive. Network managers can limit the number of simultaneous H.323 connections within their network or the amount of bandwidth available to H.323 application; and
- d. Security. H.323 addresses four general aspects of security: Authentication, Integrity, Privacy, and non-Repudiation. These are important so vendor products can provide security measures to ensure privacy for the end user and to secure the corporate or service provider networks.

SHARED OBJECTS

T.120

4. High interaction and long duration are characteristics of shared object sessions. The T.120 standard contains a series of communication and application protocols and services that provide support for real-time, multipoint data communications. Established by the International Telecommunications Union (ITU), T.120 is a family of open standards that was defined by leading data communication practitioners and is supported by Lotus, Microsoft, Intel, and many other vendors in the communications industry. The T.120 family of standards has the following benefits:

- a. Interoperability. T.120 allows endpoint applications from multiple vendors to be interoperable;
- b. Reliable, multipoint data delivery. T.120 provides an elegant abstraction for developers to create and manage a multipoint domain with ease. From an application perspective, data is seamlessly delivered to multiple parties in "real-time." Error-corrected data delivery ensures that all endpoints will receive each data transmission;
- c. Network transparency. Applications are completely shielded from the underlying data transport mechanism being used. Furthermore, T.120 supports vastly different network transports, operating at different speeds, which can easily co-exist in the same multipoint conference;

- d. Application flexibility. While T.120 includes defined whiteboarding, application sharing, and file transfer protocols, it also provides a generic, real-time communications service that can be used by many different applications; and
- e. Scalability. T.120 is defined to be easily scalable from simple PC-based architectures to complex multi-processor environments characterized by their high performance.

DCP SOP

INTRODUCTION

1. Distributed Collaborative Planning (DCP) can significantly improve overall war fighting planning processes whether in a Service, Joint, Combined or Coalition operation. By improving plan content and understanding, timeliness of plan development and objective plan assessment processes, commanders can make better and faster decisions while geographically dispersed.
2. While efficient and effective employment of DCP tools can be a force-multiplier, uncontrolled access and ill-defined procedures can result in degraded network performance, unnecessary (and excessive) bandwidth consumption, confusion, and time late information. Subsequently, DCP needs to be considered from an Information Management (IM) perspective.

AIM

3. This annex establishes the framework for planning, controlling and participating in DCP sessions to ensure maximum effectiveness and efficiency.

DESCRIPTION

4. DCP is a set of applications or tools that enable geographically dispersed members to collaborate; collaboration is the act of sharing information to develop plans collectively.

TOOLSET

5. Generally a DCP suite comprises the following synchronous and asynchronous tools and functions:
 - a. Awareness – Knowledge of who is on-line and available for collaboration;
 - b. Text Chat – Multicast or private mode chat over IP;
 - c. File Cabinet – For retention of common documents;
 - d. Bulletin Board – Interactive bulletin board in each collaborative session;
 - e. News Groups – Running discussion news group capability;

- f. Whiteboard – Persistent on-line whiteboard capability;
- g. Application Sharing – Persistent sharing of applications across the network;
- h. Screen Sharing – Persistent and dynamic sharing of an Operators screen across the network;
- i. Audio – Broadcast or private mode audio over IP;
- j. Video – Common desktop VTC;
- k. Search Engines – For visibility and retrieval of information; and
- l. Auditable – Track changes capability.

Kbps	Chat	WB	Audio	Sharing	Video
2.4	YES	POOR	POOR	NO	NO
4.8	YES	SLOW	POOR	SLOW	NO
16	YES	YES	POOR	YES	NO
32	YES	YES	YES	YES	LIMITED
64	YES	YES	YES	YES	YES
128	YES	YES	YES	YES	YES
Broadcast Type	Periodic updates	Periodic updates	Periodic updates	Periodic updates	Continuous

Table 9–B–1 Example Bandwidth Toolset Spectrum

BANDWIDTH CONSUMPTION

6. Bandwidth requirements for DCP is dependent on the particular DCP product used, the tool employed, the scalability features chosen (if available) and in cases of posting or sharing information, the file format selected. Diagram 9–B–1 depicts DCP tools relative to bandwidth consumption.

Uncontrolled copy when printed

7. Table 9-B-1 also reveals that DCP transmissions are typically of limited duration bursts. The exception is video, which is a continuous transmission. The implication is that numerous DCP sessions can often be supported if they involve burst transmissions. Diagram 9-B-2 illustrates the case in point. The use of a continuous transmission, such as VTC, will drastically increase the likelihood of network congestion, as evidenced in Figure 9-B-1.

CONFERENCE TYPES

8. The major distinctive features between DCP products are in the conferencing venue and whether the product is scalable. DCP products either employ a ‘public meeting room’ system or a private invitational system.

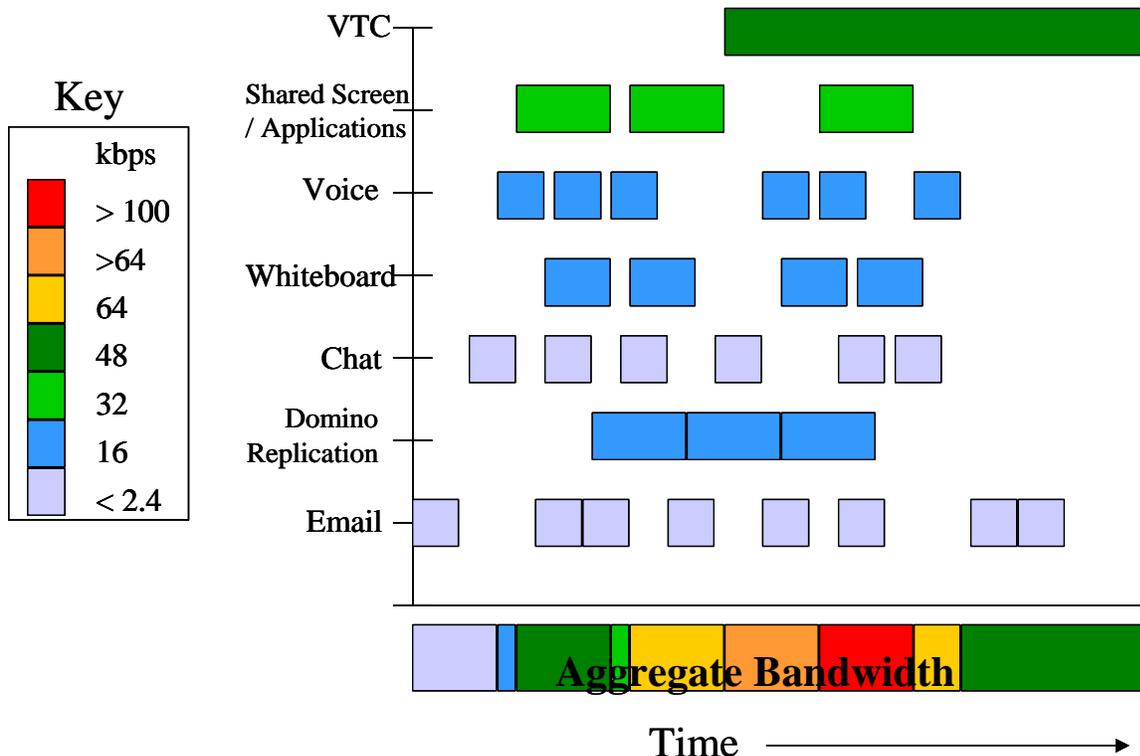


Figure 9-B-1 Bandwidth Aggregation

9. In a meeting room system members conduct collaborative sessions in meeting rooms. This system makes it easy to establish a meeting providing members have the DCP application running. Members join via a lobby or common meeting place to be informed of the location of the meeting room. Well designed buildings (a suite of conference rooms) can make knowing the location of the conference room intuitive. i.e. A meeting involving the Task Group Logistic Officers would occur in the Logistics room. This requires a dedicated DCP administrator to establish planning rooms and buildings in accordance with the Plan of Day (POD). It does mean that operational users are not required to set up, or to know, the

Uncontrolled copy when printed

communication paths or other user addresses /locations; they need only to enter a pre-defined room to start or join DCP sessions. The system can be open, in that members without invitations can listen in, unless the room is capable of being locked.

10. An invitational system is where members can only join once invited by the Session Leader. In some applications such as IBM Sametime, this can occur even if the member does not have the application open. An invite system ensures that no uninvited guests can participate.

TYPE OF PLANNING SESSIONS

11. Deliberate and ad hoc planning sessions can be conducted in either a time constrained or unconstrained environment. Ad hoc planning sessions tend to be less formalized. Collaboration can therefore occur in a formalized (scheduled and controlled) or informal setting.

USER ACCESS AND EMPLOYMENT

12. Access to DCP applications should be restricted to personnel with an operational or tactical requirement.

13. As indicated by its name, DCP is for collaborative planning. It is provided to share information of an operational or tactical nature. Common uses are to:

- a. Develop operational or tactical plans;
- b. Briefing operational or tactical plans;
- c. Brief Commanders intentions;
- d. Discuss or report situations / events as they occur; and
- e. Conduct review of plans or doctrine.

14. DCP is not provided to send personal correspondence or exchange greetings. Private use of DCP can easily result in network congestion.

ROLE-BASED ACCESS AND CONTROL

15. Users should be granted access rights for DCP tools by the system administrator on a user requirement. Figure 9-A-2 depicts the likely result where a large number of personnel would have access to chat but as the tools become more bandwidth hungry, user's access steadily declines.

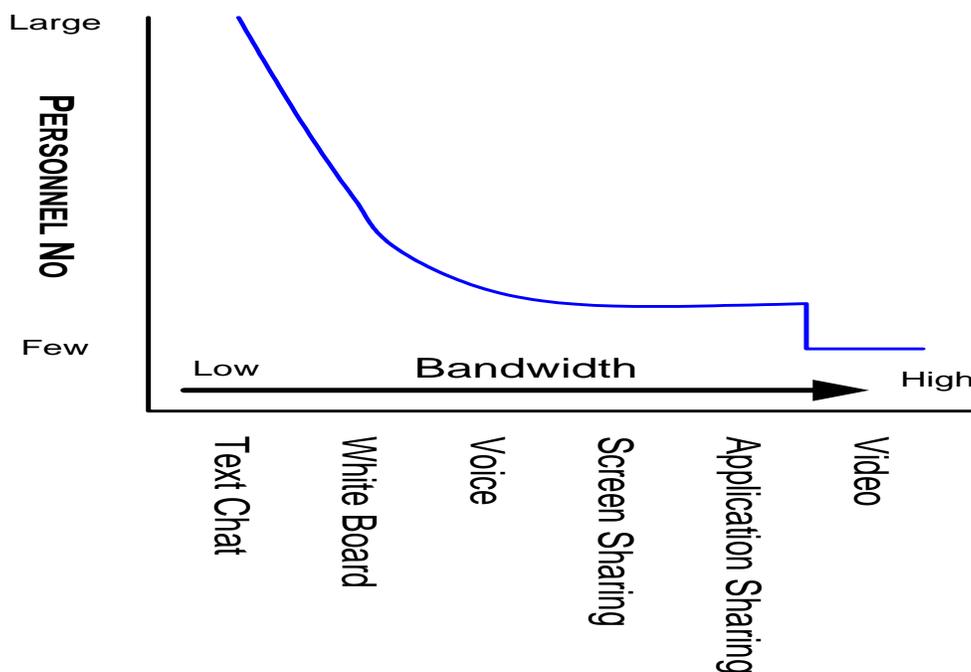


Figure 9–B–2 Operator Number Impact on Bandwidth Usage

PLANNING ORDER

16. Where possible, planning sessions should be organized in advance and reflected in the Plan of the Day (POD) or Schedule of Events (SOE). This will ensure efficient allocation of resources, especially bandwidth. Special care should be exercised to observe all normal chain of command protocols and approval procedures.

17. The benefits of informal or adhoc collaborations should be balanced against the additional bandwidth loading which could be imposed upon the network. The military commander / planner must balance time against the operational situation to determine whether to proceed in an orderly, unconstrained planning mode or in an adhoc mode. Ideally, higher bandwidth applications, especially VTC, should be left to programmed sessions.

DCP PLAN OF THE DAY

18. The CTF/CTG should develop a POD for DCP that is based on inputs from operational commanders/planners. It should be reviewed by the CTF/CTG staff. As a minimum it should include:

- a. Mission;
- b. Scenario synopsis/situation/status;

- c. Linkages to other activities or objectives;
- d. Sessions start and end times;
- e. Session Leader and alternate (different locations recommended); and
- f. Participants.

DCP PLANNING ORDER

19. The Session Leader should release a planning order which publishes:
- a. Guidance and tasking well in advance of the DCP session;
 - b. Any participants DCP constraints (i.e. unit 'x' has no VTC capability); and
 - c. What information is to be provided by whom, giving adequate notice for the type of information to be prepared?

PLANNING FOR DEGRADED DCP OPERATIONS

20. Graceful DCP degradation procedures are required in the event of communications bandwidth limitations. Typically this is accomplished by "stepping down" to less bandwidth intensive DCP tools and services.

PREDEFINED USER COMMUNITIES

21. It is recommended but not necessary that predefined user communities such as Ops Planning, Intel, C4I watch and Logistics are established to reduce administration overhead and assist coordination.

CONDUCT

AUTHORITY

22. Units are to exercise positive control over the number and type of DCP sessions conducted.

SESSION LEADER

23. The initiating participant for a planning session is the Session Leader. The Session Leader is responsible for controlling the session. A key responsibility is the management of bandwidth demand.

ESTABLISHING / JOINING A SESSION

24. To establish or join a session will depend upon whether a meeting room or invitational system is employed. In a meeting room environment all members should join the meeting place or lobby 10 minutes prior to the schedule start unless informed otherwise. For an invitational system, members should wait for an invitation. The session leader should issue the invitation 10 minutes before scheduled commencement unless briefed otherwise.

POSTING TO A SESSION

25. The use of objects in collaboration can enhance conversations. The benefits of posting material needs to be balanced by the additional bandwidth loading imposed on the network.

26. Where possible, JPEG graphic formats should be preferred over higher memory formats such as Bitmap and TIFF. Formats can be converted by using the 'save as' function and selecting a more appropriate format under the 'save as type' window.

27. Where editing is not required, Powerpoint presentations should be converted to GIF, PDF or JPEG files. This will significantly reduce the file size. At the minimum PowerPoint presentations should be saved in the 'Presentation' format rather than the other available formats.

28. All files of a large nature should be zipped. Files containing imagery should be compressed IAW OPTASK IM.

LEAVING / CLOSING A SESSION

29. Members should indicate their intention to leave a session. The Session Leader will be responsible for closing a session.

INADVERTENT LOSS OF SESSION

30. DCP sessions should be re-established as soon as possible. In a meeting room system, members should rejoin the designated room as soon as possible. For an invitational system, members will have to wait until they are re-invited.

VTC

31. Care should be taken to monitor and actively control video sessions. If left uncontrolled, video bandwidth requirements from ad hoc users could easily degrade performance of the entire DCP network, with significant reductions in data flow rates for all network users. Additionally, scalable DCP products that allow bandwidth setting should be left at the default setting unless stipulated by Command.

RECORDS

32. The Session Leader should keep a copy of any presentation given in a collaborative session. Each unit should retain a copy of all chat correspondence. All records should be retained for a minimum of two weeks, after which time they can be erased. The records should be stored in a folder specially created for holding records (with sub folders delineating days) to ensure individual records do not become misplaced. Where the Session Leader deems necessary, minutes should be made and disseminated. (Technology does not exempt the established procedures for meetings.) The use of screen capture feature (*shift+ Print Scrn*) is a useful way to record information.

TOOL SELECTION

33. DCP is most beneficial to the warfighter when the suite of DCP tools is used in combination. The most effective combination is the share program facility or whiteboarding facility used in conjunction with text and voice chat.

34. Conducting meetings relying only on text chat is tedious and slow. The conduct of meetings tends to jump around because of the slow response time. By the time a participant types a message and then sends it (especially if lengthy), the discussion will have often moved on. A better solution is to use text chat to support voice chat, i.e. the session would principally be voice but where important information was reinforced on text chat. Important information would be information other participants would want to record, such as key timings, positions and orders.

35. If a session is to be conducted principally with text chat, it is clear a procedural process is required. One recommendation, which is similar to tactical voice procedures, is that a participant indicates first he/she wants to make an entry. The first such entry which appears has the 'floor' unless the conveyer or OTC beaks in. The participant with the 'floor' would indicate completion of the transmission where the process begins again.

36. Careful consideration as to the best tool(s) to employ in a collaborative session will assist in the session's objectives being met and efficient use of bandwidth. For example, if the collaboration was to review of an OPTASK signal. This could be easily accomplished by posting the document to the homepage and using chat and if necessary voice. Text documents need not necessarily need to use the application or screen sharing tool which are more bandwidth hungry. The synchronous and asynchronous combination has been proven to be very effective. Similarly, graphics, pictures or charts need not necessarily be the sole purview of screen or application sharing tools. The homepage may be a more suitable alternative if examination is necessary prior to the collaborative session.

SECURITY

37. Normal security procedures as for any other data or voice are to be adopted.

INADVERTENT TRANSMISSION

38. Caution should be exercised with Voice and Video transmissions as unintended background discussions or classified material may be captured and broadcast. Unattended Video and Audio sessions may also constitute a security breach depending on the classification and need to know of the broadcast environment. It is recommended that headsets are used for all audio sessions.

FIREWALLS

39. Firewalls and filters should be configured to permit TCP/IP, FTP, and Multicast services transmissions. Coordination with network administrators controlling participating platforms operating behind firewalls and packet filters is required.

ENCRYPTION DATA RATES

40. Encryption equipment employed should support data rates necessary for video.

NETWORK ENGINEERING

41. As part of the DCP network planning process, the following considerations should be factored into the backbone network design:

- a. Key sites requiring redundancy;
- b. Potential single point of failures and identified work-around solutions;
- c. Specific network bottleneck locations / equipment that might impact DCP across the entire backbone network (including encryption); and
- d. Impact of various types of transmission media on DCP processes — the number of satellite hops, type of commercial landlines, packet loss etc

PRINCIPLES OF EFFECTIVE MEETINGS

42. The convenience and user friendliness of DCP does not guarantee collaborative sessions will be effective. The principles that govern effective meetings and military appreciation and planning remain as relevant and important (if not more). In fact, the ability to connect anyone with access to the network will mean that many who participate will be uneducated and inexperienced in conducting successful meetings.

43. The following general principles are worthy to consider:

- a. Employ an agenda to help control the direction of a meeting;
- b. Solicit input for an agenda and circulate the agenda well in advance; and

- c. The Session Leader should consider summarizing what has been agreed or discussed for each agenda item.

WARNINGS AND PRECAUTIONS

44. The following is a listing of warnings and precautions that network administrators should be cognizant of:

- a. **Bandwidth Loading** – DCP Network Administrators and Mission Planners should be aware of bandwidth limitations and traffic demands on the network, not only from their own DCP session tools, but also from other systems sharing the network. Network overload can result in loss of DCP capabilities, and interruption of data exchange for other network users;
- b. **Inadvertent Transmission** – Mission Planners should ensure microphones and cameras are deselected when not in use. Failure to do so will result in unnecessary bandwidth usage and may constitute a security breach;
- c. **Central Processing Unit (CPU) Loading** – Some applications are computing-intensive as well as bandwidth-intensive. It is common for a number of applications to be running at the same time. The CPU load should be monitored. If the CPU load exceeds 50%, the operator should consider shutting down some applications; and
- d. **Overuse of Action Planning** – The convenience of real-time technology combined with the awareness capability (see DCP CONOP) will increase the number of action (or impromptu) planning sessions. This will no doubt improve the dissemination of information and ideas, but if uncontrolled, it could also result in network congestion and the associate flow-on effect. Stringent user access, formalized procedures and education will avoid these problems.

TACTICAL NETWORKING COMMAND AND CONTROL TOOLS

Tool	Characteristics	Remarks	Service
Communications Planning	Is there a need for centralized network management services on C2 system. Collate OPSTAT Unit comms section for COMPLAN generation. Spectrum Planning & management desirable.	For TG & TF C2.	Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Collaboration	In accordance with ACP200B which describes in detail: - Awareness - Chat - File cabinets - Bulletin Boards - News Groups - Whiteboards - Screen Sharing - Application sharing - Audio over IP - Video Over IP - Search Engine - Office automation - Email Coalition standard appears to currently be IBM domino, including for persistent Chat. Standardised across all communities and domains.	When Bandwidth permits Video over IP is desired capability.	Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
		Need to determine what level of authentication is needed for email and chat.	Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
		Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service	
		Integration of Application / Functionality / Service	
		Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service	
		Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service	

Tool	Characteristics	Remarks	Service
COP	TG/TF must be able to contribute to COP. Surface, Sub-surface, air and land picture. Near real-time, minimal latency. Standardise symbology. Include AIS data	Still issues to resolve regards COP distribution across multiple domains – both technical as well as procedural. UK only nation not using GCCS-M/C2PC for COP. This is a separate OWG activity to address COP requirements.	Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Met and Oceanography Display & Prediction	Ability to absorb level 4 Rapid Environmental Assessment. Sensor performance prediction.		Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Coalition Fire Planning		Wider requirement of joint fires requirements of a JTFC required. Standardised tool being assessed in TW07	Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Mapping, Charting & Geodesy		To include wide range of graphics for mission planning. Need to define agreed mapping standards – specialist advice required from Land. Understand that ABCA have recently agreed	Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service

Tool	Characteristics	Remarks	Service
		standard. Requires set of graphical tools for planning purposes. Especially important for Littoral Ops.	Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
ATO Planning	Receive and display ATO. Assume TG/TF will assume CAOC role. Airspace Planning. Air Mission Planning.	NATO & CENTRIXS uses TBMCS. Compatibility issues exist.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Logistics Planning		Quadrilateral Logistics Forum are pushing logistics tool – review for CTG/CTF log planning requirements.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Imagery & Video Management	Provide audit trail for video image changes.	XN View is being trialed in TW07.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
			Provision of Application / Functionality / Service Integration of Application / Functionality / Service

Tool	Characteristics	Remarks	Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
ORBAT Manipulator	?????????? Own & OPFOR.	Maintaining data base is expensive & time consuming.	Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
JMAP/Appreciation/Operational Planning Process.	COA & alternative action Analysis COA Wargaming Mission Simulation & Replay Mission Analysis Exercise & Training Simulation Mission Upload/download Operational Analysis	We may need to investigate standardised tools across Allied Forces.	Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Route Planning	Maritime & Air UNCLOS information required Q-Route AWNIS Air Routes		Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service
			Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Network Management	Tiered Network management tools.		Provision of Application / Functionality / Service
			Integration of Application / Functionality / Service

Tool	Characteristics	Remarks	Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
INTEL Analysis	Access to intelligence products.	Janes on-line perhaps.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Briefing Tools	NXP Lite required for file compression to minimise to bandwidth consumption.	There has been wider proliferation of MS Office products. This requirement should be revalidated. ACP200 discusses use of PowerPoint.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Calendaring		Planned for CENTRIXS CAS3.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Directory Services	Global address list that can be searched, with standardised entries.		Provision of Application / Functionality / Service Integration of Application / Functionality / Service

Tool	Characteristics	Remarks	Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Document Management System		Important core service requirement for C2 system. CAS is attempting to achieve this through process.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Integrated Messaging System	This would be email and chat that complies with characteristics in CONOPS for Tactical Messaging.		Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Office Automation		There has been wider proliferation of MS Office and it is assumed that this will be standardised product, for the immediate future Office 2003.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Web Browser	Standard COTS browser with regular Updates.		Provision of Application / Functionality / Service Integration of Application / Functionality / Service

Tool	Characteristics	Remarks	Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Workflow Application		Lotus provides for workflow management. This requirement should be revalidated in terms of the degree to which Lotus, in conjunction with MS Office products, satisfies this requirement. Inconsistent use across the Coalition; requirement needs to be validated.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Tactical decision aids	Screen planning MCM Planning & Evaluation Amphibious Planning	Does the AUSCANNZUKUS want to determine such applications.	Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Force Readiness State	Provide near real time presentation of readiness status of Force Elements/Units.		Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
Water Space Management	Subs/MPA		Provision of Application / Functionality / Service Integration of Application / Functionality / Service

Tool	Characteristics	Remarks	Service
			Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
RFI	Means to manage RFI.		Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service
			Provision of Application / Functionality / Service Integration of Application / Functionality / Service Provision of Infrastructure / Hardware Devices (Pervasiveness and Access) to support Application / Functionality / Service Provision of Communications Infrastructure / Network Connectivity to support Application / Functionality / Service

TABLE 9-C-1 TACTICAL NETWORKING COMMAND AND CONTROL TOOLS

GLOSSARY OF TERMS**ACRONYMS**

ACIXS	Allied Communication Information Exchange System
ACL	Access Control List(s)
ACP	Allied Communications Publication
ADNS	Automated Digital Network System
ALE	Automatic Link Establishment
ARQ	Automatic Repeat Request
AS	Autonomous System
ASN	Autonomous System Number
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code Information Interchange
ATM	Asynchronous Transfer Mode
ATO	Air Tasking Organisation
AUS	Australia
BER	Bit Error Rate
BERT	Bit Error Rate Test
BIND	Berkeley Internet Name Domain
BGP	Border Gateway Protocol
BLOS	Beyond Line of Sight
BPD	Boundary Protection Device
CA	Canada
CAP	Channel Access Processor
CAR	Committed Access Rate
CAS	Collaboration At Sea
CATF	Commander Amphibious Task Force
CBWFQ	Class Based Weighted Fair Queuing
CCEB	Combined Communications-Electronics Board
CCI	Controlled Cryptographic Item
CELP	Code Book Excited Linear Predictive

CENTRIXS	Combined Enterprise Regional Information Exchange System
CFE	CENTRIXS Four Eyes
CFLCC	Coalition Force Land Component Commander
CFMCC	Coalition Force Maritime Component Commander
CIDR	Classless Inter-Domain Routing
CIK	Crypto Ignition Key
CJTF	Commander Joint Task Force
CODS	Coalition Data Server
CONOPS	Concept of Operations
COP	Common Operational Picture
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off The Shelf
COWAN	Coalition Operations Wide Area Network
CQ	Custom Queuing
CRIU	CAP to Router Interface Unit
CST	COP Synchronization Tool
CSU	Crypto Support Unit
CT	Cipher Text
CTF	Commander Task Force
CTG	Commander Task Group
CWAN	Coalition Wide Area Network
CWC	Composite Warfare Commander
DAC	Discretionary Access Control
DAMA	Demand Assigned Multiple Access
DBS	Direct Broadcast Service
DCP	Distributed Collaborative Planning
DNS	Domain Name Service
DTD	Data Transfer Device
DVMRP	Distance Vector Multicast Routing Protocol
EKMS	Electronic Key Management System
ELOS	Extended Line of Sight

EMCON	Emission Control
EoS	Elements of Service
FF	Fire Fly
FIFO	First In, First Out
FOTC	Force Over The Horizon Track Coordinator
FTP	File Transfer Protocol
GBS	Global Broadcast System
GCCS-M	Global Command Control System – Maritime
GCTF-1	Global Coalition Task Force One
GEM	General Dynamics Encryptor Management
GOTS	Government off the Shelf
GUI	Graphical User Interface
HAG	High Assurance Guard
HDR	High Data Rate
HF	High Frequency
HIT	High Interest Track
HSD	High Speed Data
HTML	Hyper Text Mark-up Language
HTTP	Hyper Text Transport Protocol
IANA	Internet Assigned Numbers Authority
ICE	Imagery Compression Engine
IDM	Information Dissemination Management
IDP	Information Dissemination Plan
IGMP	Internet Group Management Protocol
IIS	Internet Information Service
IM	Information Management
IMI	Information Management Infrastructure
IMAP	Internet Message Access Protocol
IMPP	Instant Message and Presence Protocol
INE	In-line Network Encryptors
INMARSAT	International Maritime Satellite Organisation

IP	Internet Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
IWC	Information Warfare Commander
IXS	Information eXchange System
JCSS	Joint Command Support System (Australia)
JMUG	JMCIS Multicast Gateway
KMID	Key Management Identification
LAN	Local Area Network
LDAP	Light Directory Access Protocol
LES	Land Earth Station
LMD/KP	Local Management Device / Key Processor
LOS	Line of Sight
LSA	Link State Advertisements
MAC	Media Access Control
MAG	Maritime Air Group
MCAP	Medium Data Rate Channel Access Processor
MCOIN	Maritime Command Operations Information Network (Canada)
MDP	Multicast Dissemination Protocol
MDR	Medium Data Rate
METOC	Meteorological/Oceanographic
MFTP	Multicast File Transfer Protocol
MMF	Multi-National Marine Force
MNTG	Multi-National Naval Task Group
MOSPF	Multicast Open Shortest Path First
MPLS	Multi-Protocol Label Switching
MSAB	Multinational Security Accreditation Board
MSeG	Multicast Service Gateway
MSL	Multi- Security Levels
MTA	Message Transfer Agent
MTWAN	Maritime Tactical Wide Area Network

NBAR	Network-Based Application Recognition
NCW	Network Centric Warfare
NES	Network Encryption System
NM	Network Management
NNTP	Network News Transport Protocol
NOC	Network Operations Center
NRS	Naval Radio Station
NZ	New Zealand
OPCON	Operational Control
OPGEN	Operational General Messages
OPTASK	Operational Tasking Messages
OSI	Open System Interconnect
OSPF	Open Shortest Path First
OTCIXS	Officer in Tactical Command Information eXchange System
PAD	Packet Assembler Disassembler
PC	Personal Computer
PCM	Pulse Code Modulation
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
PLAD	Plain Language Address Designator
P_MUL	Protocol Multicast
POP3	Post Office Protocol Version 3
PPK	Pre-Placed Keys
PPP	Point-to-Point Protocol
PQ	Priority Queuing
PT	Plain Text
QOS	Quality of Service
RED	Random Early Drop
RIP	Routing Internet Protocol
RF	Radio Frequency
RP	Rendezvous Point

RSVP	<i>Resource ReSevation Protocol</i>
RTF	Rich Text Format
RTT	Round-Trip Time
SHF	Super High Frequency
SIPRNET	Secret Internet Protocol Router Network (United States)
SMG	Secure Mail Guard
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNR	SubNet Relay
SOPS	Standard Operating Procedures
TBS	Theatre Broadcast Systems
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEK	Transmission Encryption Key
TG	Task Group
TGAN	Task Group Area Network
TOIS	Technical Operating Instructions
TOS	Type Of Service
TTL	Time To Live
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UID	Unit Identifier
UK	United Kingdom
US	United States
USS	United States Ship
VHF	Very High Frequency
VPN	Virtual Private Network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Dropping
Z	Cryptographic Device

LIST OF EFFECTIVE PAGES

Subject Matter	Page Numbers
Title Page	i
Forward	ii
Letter of Promulgation	iii
Record of Message Corrections	iv
Table of Contents	v to xi
List of Figures	xii to xiii
List of Tables	xiv
Chapter 1	1-1 to 1-4
Chapter 2	2-1 to 2-10
Chapter 3	3-1 to 3-14
Annex A to Chapter 3	3A-1 to 3A-6
Annex B to Chapter 3	3B-1 to 3B-3
Annex C to Chapter 3	3C-1 to 3C-4
Annex D to Chapter 3	3D-1 to 3D-4
Chapter 4	4-1 to 4-11
Chapter 5	5-1 to 5-3
Chapter 6	6-1 to 6-7
Annex A to Chapter 6	6A-1
Chapter 7	7-1 to 7-6
Annex A to Chapter 7	7A-1 to 7A-11
Chapter 8	8-1 to 8-10
Annex A to Chapter 8	8A-1 to 8A-6
Annex B to Chapter 8	8B-1 to 8B-4
Annex C to Chapter 8	8C-1 to 8C-6
Chapter 9	9-1 to 9-7
Annex A to Chapter 9	9A-1 to 9A-3
Annex B to Chapter 9	9B-1 to 9B-10
Annex C to Chapter 9	9C-1 to 9C-8
Glossary of Terms	Glossary-1 to Glossary-6
List of Effective Pages	LEP-1

Uncontrolled copy when printed

UNCLASSIFIED

ACP 200(C) Vol 1

ACP 200(C) Vol 1

Uncontrolled copy when printed

UNCLASSIFIED