7th International Command and Control Research and Technology Symposium

Interoperability – An Australian View

Neil Warner
ADI Limited

neilwarner@uunet.com.au

Abstract

Australia's traditional allies have been New Zealand, UK and USA. Before the advent of digital C3I Systems, interoperability between Australian, US and UK forces was maintained by the use of common communications equipment and procedures but also by the use of people, training and doctrine. Further, Australia has traditionally procured from the US or UK C3I major military equipment purchases, including C3I systems. This assured some level of interoperability with US and UK forces.

From the viewpoint of the past decade, it is clear that the majority of future operations of the Australian Defence Force will be Operations Other Than War. This will require the Australian Defence Force to operate in coalitions or alliances. The partners within these coalitions or alliances may not have common doctrine, training or operating procedures. Security will also be a major issue. The operational environment within these partnerships will also need to take into account civil and national influences, as well as influence from UN participation or control as well as various Non Government Organizations (NGOs) that are heavily involved in these operations.

Interoperability can be defined as the ability of systems, units or forces to provide to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together. Interoperability cannot solely be thought of on an information system level, but must include doctrine, people, procedures and training.

This paper will examine interoperability of Command and Control Systems (C3I), with reference to the Australian Defence Force. The paper will include a discussion of the technical concepts of interoperability, as well as an examination of ADF requirements and it's current status. A review of outstanding issues will also be included.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
SEP 2002		**00-00-2002 to 00-00-2002**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Interoperability - An Australian View	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ADI Limited,Locked Bag 3000,Potts Point NSW 2011,Australia, ,**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**15**	

Introduction

Australia's traditional allies have been New Zealand, UK and USA. Before the advent of Digital C3I Systems, interoperability between Australian, US and UK forces was maintained by the use of common communications equipment and procedures and also by the use of people, training and doctrine. Australia has a long history of training with military forces in the UK and US and also participating in Exchange of personnel. This has allowed Australia to interoperate with US and UK forces as the Commanders tended to think the same way and with similar procedures, due to large amount of training and interaction the commander and their staff would have had with similar NZ, UK and US commands and HQs.

Further, Australia has traditionally procured from the US or UK C3I major military equipment purchases, including C3I systems. This assured some level of interoperability with US and UK forces providing Australia was prepared to accept that the nature of these foreign sourced systems reflected the source county's unique requirements and "eyes only" restrictions. In recent times, the Australian military has not always procured systems from US and UK forces, and has developed systems within Australia by Australian Industry.

From the viewpoint of the past decade, it is clear that the majority of future operations of the Australian Defence Force will be operations other than war. This will require the Australian Defence Force to operate in coalitions or alliances not only with US forces, but with forces and non-military organisations of many other countries. The partners within these coalitions or alliances may not have common doctrine, training or operating procedures. Security may also be a major issue. The operational environment within these partnerships will also need to take into account civil and national influences, as well as influence from UN participation or control as well a various Non Government Organizations (NGOs) that are heavily involved in these operations.

The essence in these situations is that interoperability is required with all participants in the coalition or alliance, and this requires the ability to integrate command, control and especially communications systems within this coalition or allied organizational structure. This will include the need to share and exploit common information.

Aim

This paper will examine interoperability of Command and Control Systems (C3I), with particular reference to the Australian Defence Force. The paper will include a discussion of the technical concepts of interoperability, as well as an examination of ADF requirements and it's current status. A review of outstanding issues will also be included.

Definitions

"Alliance" – A formal agreement between countries especially referring to a military relations. Australia's allies are generally referred to as the AUSCANNZUKUS being Australia, Canada, New Zealand, United Kingdom and USA.

"Coalitions" – An alliance between groups, parties or countries especially for some temporary of specific reason.

“Operations Other Than War (OOTW)” - includes peace operations, as well as a wide range of other non-traditional military operations. The U.S. Army's Field Manual 100-5[1] defines OOTW as consisting of "support to U.S., state, and local governments, disaster relief, nation assistance, drug interdiction, peacekeeping, support for insurgencies and counterinsurgencies, noncombatant evacuation, and peace enforcement." Peace operations, particularly those conducted under the auspices of the UN Charter, have become more common in the post-Cold War world.[2] In the post September 11 world, this would include counter terrorism aspects as well.

“Interoperability” – The ability of systems, units or forces to provide to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.[3]

Technical Concepts of Interoperability

General

Interoperability can be defined as the ability of systems, units or forces to provide to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together. Interoperability cannot solely be thought of on an information system level, but must include doctrine, people, procedures and training. It is intended to concentrate with this section of the technical requirements of the information system.

Within the last five years, the technical concepts of interoperability have been defined in initially with the Levels of Information Systems Interoperability (LISI) from the US DOD C4ISR Architectural Working Group and Combined Interoperability Technical Architecture (CITA) (ACP140) from the CCEB.

Discussion below will be undertaken of current approaches and future initatives in technical level of interoperability.

Formatted Messages

Formatted messages provide a standard method of transmitting selected information between different systems. These are normally referred to as Message Text Formats (MTF) and are character-based representation of information that are human readable. Formatted messages are used as an interface data protocol between dissimilar information systems. An example of a message (without transmission envelope) is below:

```
MSGID/MIC SYDNEY/GOLD/05685/JAN
CTC/ASSHEP/PALUMA-SHEPPARTON//AGSC/NAV/03/AS
POS/020530Z0/JAN/1651S3/14543E7//000T/001NM/001NM
ARR/CAIRNS/AS/020530Z0/JAN
ENDAT/DECL: OADR
```

[1] [US Army FM 100-5, 1993]
[2] [ACT, 1995]
[3] [ADFP 101]

Example 1 – OTG Contact Report[4]

These messages can be transmitted on a variety of communications systems, from teletype systems using Baudot encoding to complex modern information systems using email or TCP Sockets as the transmission medium.

These messages represented the first attempt at a standard for interoperability between information systems. Formatted message are still in very common use and are probably the most common form of implementing interoperability current in force within Australia or with alliances or coalitions. The following standards are commonly in use within Australia or would affect Australia:

- ADFORMS – Australian Defence Formatted Message System
- OS-OTG or Gold Message – US Naval Standard and in very common use within Australia
- ADatP-3[5] – NATO Message Text Formatting System (FORMETS)

Levels of Information Systems Interoperability (LISI)[6]

Introduction

Levels of Information Systems Interoperability (LISI) is a US DOD initiative. It flows on from the development of the Joint Technical Architecture (JTA)[7], the Defense Information Infrastructure (DII) Common Operating Environment (COE)[8] and the C4ISR Architectural Framework[9]. US DOD lacks a formal construct that addresses different levels of information-exchange and interoperability sophistication and LISI was the way one way ahead, but not the only, to assist in remedying this situation.

The LISI Capability Model defines a series of level for interoperability s summarized below.

Level 0 Isolated Interoperability in a Manual Environment

Level 0 encompasses the wide range of isolated, or stand-alone, systems. No direct electronic connection is allowed or is available, so the only interface between these systems is by manual re-keying or via extractable, common media. Fusion of information, if any, is done off-line by the individual decision-maker by other automated means.

---

[4] [OS-OTG, 1999]
[5] [ADatP3, 2001]
[6] [LISI, 1998]
[7] [JTA, 2000],
[8] [DIICOE, 2000]
[9] [C4ISR AWG, 1997]

Level 1 Connected Interoperability in a Peer-to-Peer Environment

Level 1 systems are capable of being linked electronically and providing some form of simple electronic exchanges. These systems have a limited capacity, generally passing homogeneous data types, such as voice, simple "text" e-mail, or fixed graphic files such as GIF or TIFF images between workstations. They allow decision-makers to exchange one-dimensional information but have little capability to fuse information together to support decision-making.

Level 2 Functional Interoperability in a Distributed Environment

Level 2 systems reside on local networks that allow data sets to be passed from system to system. They provide for increasingly complex media exchanges. Formal data models (logical and physical) are present. Generally, however, only the logical data model is accepted across programs and each program defines its own physical data model. Data is generally heterogeneous and may contain information from many simple formats fused together, such as an image with an annotated overlay. Decision-makers are able to share fused information between systems or functions.

Level 3 Domain-Based Interoperability in an Integrated Environment

Level 3 systems are capable of being connected via wide area networks (WANs) that allow multiple users to access data. Information at this level is shared between independent applications. A domain-based data model is present (logical and physical) that is understood, accepted, and implemented across a functional area or group of organizations that comprises a domain. Using agreed-upon domain data models, systems must now be capable of implementing business rules and processes to facilitate direct database-to-data-base interactions, such as those required to support database replication servers. Individual applications at this level may share central or distributed data repositories. Systems at this level support group collaboration on fused information products. Decision-making is supported by fused information from a localized domain.

Level 4 Enterprise-Based Interoperability in a Universal Environment

Level 4 systems are capable of operating using a distributed global information space across multiple domains. Multiple users can access and interact with complex data simultaneously. Data and applications are fully shared and can be distributed throughout this space to support information fusion. Advanced forms of collaboration (the virtual office concept) are possible. Data has a common interpretation regardless of form, and applies across the entire enterprise. The need for redundant, functionally equivalent applications is diminished since applications can be shared as readily as data at this level. Decision-making takes place in the context of, and is facilitated by, enterprise-wide information found in this global information space.

Combined Interoperability Technical Architecture (CITA) ACP 140[10]

The CITA is a Combined Communications-Electronic Board (CCEB) nations[11] initiative, separate from the US DOD LISI initiative.

The CCEB observed that the operational environment of the future is perceived to be one of coalitions, flexible in their constitution and unlikely to be constrained to CCEB members. Partners will not have common procedures and operational techniques. The operational environment will also need to take into account civil and national influences and the integration of functional elements at all levels of the organizational structure.

The essence of combined interoperability was seen as the ability to integrate command and control systems within this coalition structure. This requirement is the ability to share and actively exploit common information while dynamically developing processes and procedures that are appropriate to the existing coalition.

The CCEB vision statement adopted by the Principals which describes the goal environment is:

"The CCEB is committed to maximizing the effectiveness of combined operations by the definition of a Combined Interoperability Environment. This environment will enable users to share, creatively apply and add value to collective information and knowledge, constrained solely by policies defined by originators and recipients."

Detailed below are the levels defined with the CITA document.

Inter. Level	Name	Description
1A	Basic Document Exchange	OA document interchange, hypertext, character sets/alphabets, graphics/still and moving images, file compression, page description, security labeling, accounting and audit.
1B	Full document exchange	As for 1a plus military transfer formats, military symbols (codes only) and standard data products.
2A	Network Connection	Inter-networking, transport and domain name services.
2B	Basic Intranet Connection	File transfer and interpersonal email with attachments.
2C	Web connection	Hypertext transfer, on-line publishing and news group services. Security labelling syntax, semantics and positioning within published documents. Also web authentication and access control mechanisms.
2D	Organisational Messaging	Organisational messaging based on X.400 as defined in ACP 123. Also messaging security services.
2E	Directory Services	Directory services based on X.500 as defined in ACP 133.
3A	Secure database access/exchange	Database management, remote database access, data dictionary, CCEB data model and associated security services.
3B	Distributed applications	Distributed computing, object interfaces and object middleware if relevant. Also database replication, information sharing, collaborative computing and special applications.

Table 1- CITA Level of Interoperability

[10] [CITA, 1999]
[11] CCEB nation are Australia, USA, United Kingdom, Canada and New Zealand.

Way Ahead

Formatted messages are in common use at the current time and it is thought that they will in use for the foreseeable future, and will provide a low technology but highly reliable solution for interoperability. This solution is most applicable to the Coalition and Allied situation as it requires low technology and the character-based nature of the interface data protocol make security filters between national systems and security levels easier to implement (e.g. US DOD Radiant Mercury, which was used in JWID exercises as a "Dirty Word" checker).

LISI and CITA documents not only define the technical requirements for interoperability but also provides levels of interoperability that provide a maturity model for and a process for determining joint interoperability needs, assessing the ability of our information systems to meet those needs, and selecting pragmatic solutions and a transition path for achieving higher states of capability and interoperability. Although the levels defined in LISI and CITA do not directly correspond, their intention and end results are for practical purposes identical. Both these models can be used later within this paper to examine and analysis the ADF current position with respect to it national systems, and interoperability with Allies and Coalitions.

The most recent initiative within interoperability is the Multilateral Interoperability Program (MIP[12]). The aim of MIP is to achieve international interoperability of Command and Control Information Systems (C2IS) at all levels from corps to battalion, or lowest appropriate level, in order to support multinational, combined and joint operations and the advancement of digitization in the international arena including NATO. To this end, this program will make maximum use of the operational, procedural and technical work previously undertaken within the Quadrilateral Interoperability Program (QIP), the Battlefield Interoperability Program (BIP) and the Army Tactical Command and Control Information System (ATCISS), as well as seeking closer co-operation with similar programs.

The current aim is to agree doctrine and develop concepts for interoperability. The initiative is it's early stages, but has too current objectives for interoperability:

- MIP Phase 1 – Interchange of Formatted messages derived from the MIP Common Data Model (MCDM) but with MTFs based on ADatP-3 Version 12.
- MIP Phase 2 - To define and develop a (push) data capability that implements a fieldable automated data exchange capability supporting vertical and horizontal interoperability.

MIP nations are Canada, France, Germany, Italy, United Kingdom, USA plus observers nations including Australia, Austria, Belgium, Denmark, The Netherlands, Spain. However, the status of the observer nations may have changed, as it is believed that Australia may have agreed to join as a full member. This will certainly have an effect on future Australian interoperability implementations, especially on Land based systems but could also have effect on Joint, Maritime and Air base C3I Systems.

[12] [MPMP, 2002]

Australian Defence Force Requirements

Statement of Requirements

From Defence Australia[13], interoperability is seen as an essential requirement as part of Australia's Alliance with the US and Australia's ability to work with Allies in a Coalition, as shown in the three extracts below:

The Government expects that these forms of practical cooperation will continue to grow over coming years. Technology offers new opportunities to work together, and to deepen cooperation in many areas. It also provides new imperatives to achieve closer integration and interoperability of capabilities and systems. In an era of high technology warfare, effective alliances will need systems that can operate at a level of detail in real time. Those systems will need to be built in peacetime if they are to be of value in a crisis.

The same factors place a premium on interoperability between our forces and countries with whom we might want to operate in coalition. The development of interoperability - within limits of cost and other factors - is an important issue in capability development.
…….

The Government's aims for Information Capabilities are to position the ADF to harness advances in information technology in ways that ensure that the ADF has timely, accurate and secure information to exploit fully individual and unit combat capabilities, and allow their employment in more flexible ways. Our specific objectives include:
…….

Ensuring these systems are managed effectively, secure against information warfare attack and able to achieve a high level of interoperability with our allies and partners.
…….

This demonstrates that the ADF and it political masters put an emphasis on working in alliances and coalitions as part of the basic strategy operation premise of Australia's defence operations. This can only come about when interoperability between operation units can be achieved, and this would include information and command control and support systems.

Analysis of Requirements

Interoperability is a multi-level concept and there are requirements for interoperability between:

- All levels of war – Tactical, Operational and Strategic;
- Between C3I Systems designed for different purposes;
- Services and or Environment – Land, Air and Maritime;
- Military and Civilian Authorities.

[13] [Defence Australia, 2000]

The extracts above from Defence Australia, assume and imply that interoperability within Australian systems has already been established, which may not be the case. This will be discussed more fully below.

The implementation of full interoperability is not always required or desirable. This concept stems mostly from security issues. The interoperability requirements should be tailored for different missions as interoperability functional can significantly add complexity and cost to the implementation of a system.

National Systems should strive to obtain the highest level of interoperability (LISI level 4 CITA 3B). Australia's National systems Joint Command Support Systems (JCSS), Air Command Support System (ACSS), Mine Warfare Command Support System (MWCSS), MCSS and Battlefield Command Support System (BCSS) should obtain this level. However, obtaining this level would in reality be the requirement for one System, or Systems of Systems, with a central core and many different applications to suit the requirements of the wide variety of Users Type. This is what is currently being proposed as the ADF attempt to migrate all command support systems to one core, currently called Joint Command Support Environment (JCSE).

Where Australia participates with it's allies, in particular the AUSCANUSNZUK Nations (CCEB Nations) then the requirements are somewhat different, depending on the mission involved. A lower level of interoperability may be more palatable in this case as the observation and control of the transfer of information can be implemented. It is viewed that LISI level somewhere between Level 2 and Level 3 or CITA 2A to 2E is the desirable level.

Australian Defence operation over the last 10 years have mostly but not exclusive been concerned with Peacekeeping or humanitarian assistance, which has been grouped into the Operations other than War (OOTW) category. Within this type of operation, Australia defence units need to interoperate not only with other units within the coalition undertaking the operation but also with civilian and other NGOs providing the humanitarians relief. Interoperability with UN organizations is also a requirement. Both these requirements are challenging due to the security implications.

Implementation of ADF Interoperability

Australian Systems

Where one would expect a very high level of interoperability in Command Support System used within the ADF, these have been designed and development with very little or no levels of interoperability. While the JCSS and ACSS share a common architectural basis and therefore provide some level of interoperability, with exchange of files, images and email commonplace and Web technology is also used. Theatre Battle Management Core System (TBMCS) has been included with ACSS and exchange of situation awareness information has been implemented using formatted messages.

Interoperability between JCSS and ACSS and BCSS is rather more problematic. BCSS when deployed in the field uses a COTS Package called “CDNS-A” which communicates via a propriety protocol across Combat Net Radios (CNR). When installed on a LAN within a Headquarters, these propriety messages are still used but across a LAN based TCP interface. Interoperability using the exchange of situation awareness information is still problematic and information flows via formatted messages are only implemented from BCSS to JCSS. Transfer of other information from BCSS to JCSS is via email and replication of databases but this only takes place at the Brigade HQ Level.

Interoperability with Allies and Coalitions

Interoperability with Australia allies (AUSCANUSNZUK Nations) has always been well founded as Australia has traditionally used both US and UK sources equipment (as has New Zealand and Canada) and therefore not only technical but operation interoperability has been easily achieved. In recent times the ADF has not always procured C3I systems from US and UK sources, and has been actively developing systems with Australia. These systems (eg. JCSS) have always stressed the need for interoperability with US systems and they have been designed and implemented with these requirements in mind. The type of interoperability is still based on formatted message passing, and the use of email and internet type connectivity. The reason this has remained at this level is that security issues still result in restrictions to full interoperability. Australia implements an “AUSTEO” (Australian Eyes Only) caveat and US has NOFOREYES “No Foreign Eyes” caveat. These caveats reduce the possibility for increased levels of interoperability.

Currently, most Australian systems operate at the Secret Level, while UN and Coalitions due to the nations involved, operate at the Restricted Level. NGO and other such organizations operate at an Unclassified level and generally utilize the Internet for communications. Different security levels as discussed above will always act as an impediment to interoperability.

Joint Warrior Interoperability Demonstration

JWIDs are US Joint Staff-sponsored demonstrations of evolving C4ISR technologies and Joint and Combined Forces interoperability solutions.

JWIDs are run as exercises, where "demonstrations" have to perform before users who are attempting to use them in real world situations.

In Australia, JWID has developed into an activity focused on[14]:

- Enhancing Joint and Combined Interoperability between national systems.
- Capability development, including policies, procedures and doctrine.
- Exploring future concepts.
- JWID is a key forum to influence the development of the emerging Combined Information Environment.

Australia has been participating in JWIDs since 1995. The participation by Australia, both at the Defence level and industry level gives the opportunity to test existing systems and also new concepts and capabilities in a semi-exercise situation. These are invaluable for testing interoperability concepts within an operational scenario.

Within JWID 2002, interoperability of Command Support Systems was a major aspect of the Australian effort in the exercise. The main Australian JWID2002 aim was to demonstrate interoperability between Australian operational and tactical level command support systems and between Australian command support systems and US command support systems. The demonstration was to investigate interoperability between different command support systems in both a joint and coalition context showing that technology developments and emerging standards are removing the perceived need to acquire identical systems to ensure interoperability. Interoperability was achieved via a number of methods including:

- Passing of formatted messages, including OTG[15] and Coalition Information Exchange (CIX)[16] format;
- Sharing of Data through common accessed Web Servers;
- Fusion of data available in commonly accessed databases and web servers.

Both a technical and operational evaluation was conducted.

The architecture of the demonstration is shown in Figure 1 below. The operational concept was to impose an Australian system between two US Systems, as the role of the Land Component Commander (LCC) was undertaken by Australia. The LCC wanted to utilize the system that the LCC and staff were familiar with namely the Australian JCSS. However, the LCC had subordinate commands that were made up of units from other nations, including US, Australia Spain and others. GCCS and other systems were used at this level.

[14] [JWID, 2002]
[15] [OS-OTG, 1999]
[16] [CIX, 2002]

The initial evaluation indicated that the system did provide a high level of interoperability for a limited set of message types. This activity did indicate areas of deficiency and areas were improvements could be made to increase operational capabilities. The JWID demonstrations are an important activity to prove or demonstrate what levels of interoperability can be achieved and how this can be accomplished.

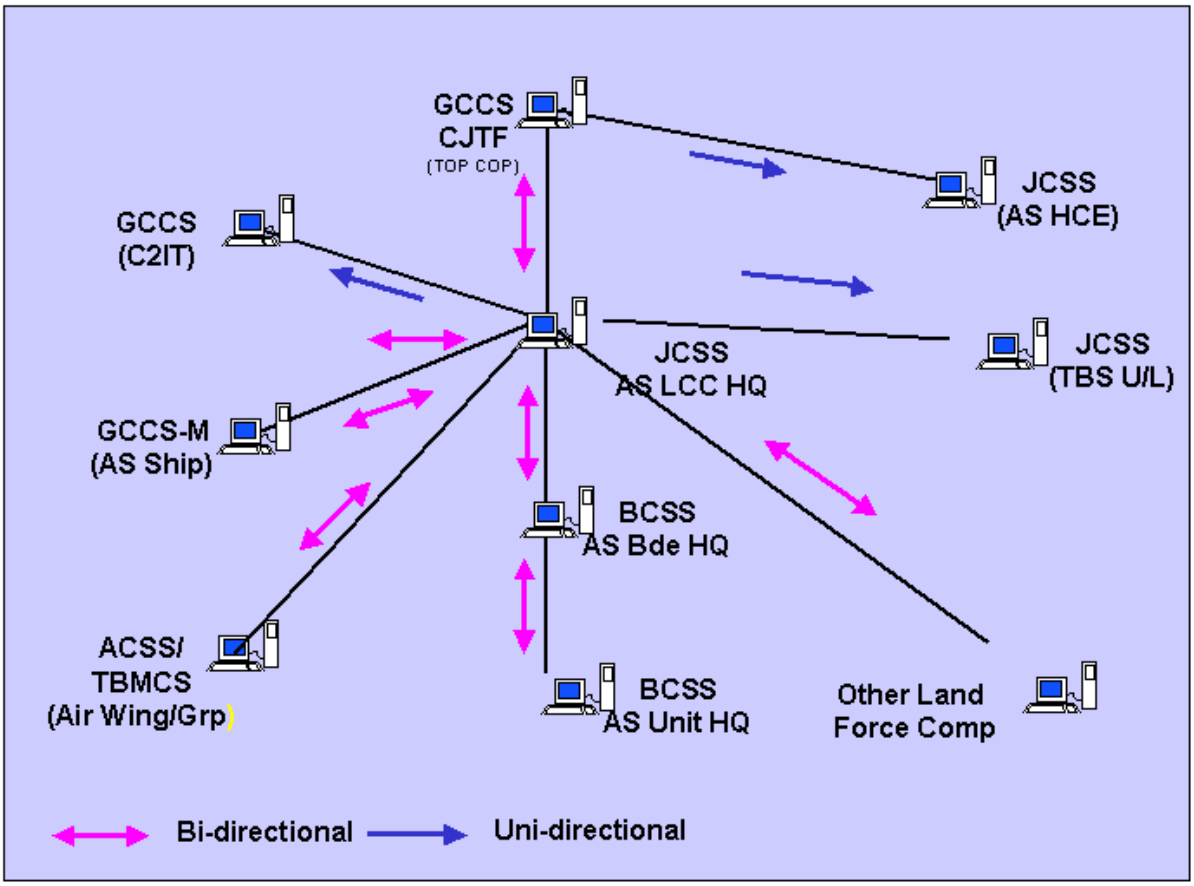

Figure 1 – JWID 2002 Interoperability Demonstration

Current Initiatives

Australia and the US are participating in a technology demonstrator program with the aim of overcoming the security problems to some extent. The current initiative is called "Coalition Theatre Logistics Advanced Concept Technology Demonstrator (ACTD)"[17]. The aim of this ACTD is to share accurate logistics information with coalition partners for the full spectrum of military operations. The technical concept is to provide an information island, populated from individual national systems, from which coalition information can be accessed through web browsers or similar technology. This is shown in Figure 2 below:

[17] [CTL ACDT, 2001]

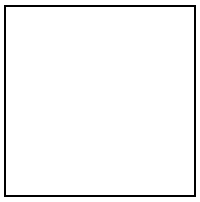

Figure 2 – Coalition Theatre Logistics Architectural Overview

Transfer of data to and from the "information islands" would be through gateways implementing national security policy. This concept, although in it early stages of implementation, offers great promise in solving some of interoperability issues caused by security. This will be trialled in Joint Warrior Interoperability Demonstration (JWID) 2002, which was discussed earlier in this paper.

Outstanding Issues

Security is always and still is the major outstanding issue when discussing interoperability. Whether discussing interoperability between national systems or interoperability between allied or coalition system's security is still the major restricting issue.

During Australia's recent and current involvement in East Timor, during Operation Stabilize and Warden, security was the most limiting factor for interoperability within the coalition. A common information system has established for command and control and command support, but due to the security policies of nations within the coalition, this system only operated at the Restricted Level. At this level, intelligence information and operation planning information was not hosted on this system, but within national enclaves that were separated from the common coalition system. This one of the major limiting factors within the conduct of the operation

The issue of national security will not one that will be easily overcome. The requirement for need to know in national systems works against the "all informed" concept with most Information Systems and therefore restricts the limits to which interoperability can be applied.

The advent of Multi Level Secure Systems should be able to eliminate to some extent this problem. In addition, the introduction and use of trusted data diodes and transfer mechanisms should reduce this problem. However, both these technologies have been discussed for some years and no real implementations exist that would assist in solving this problem.

Conclusion

The Australian Defence Force will need to operate in coalitions or alliances in traditional defence of Australia or OOTW Roles. Interoperability within national systems is required as well as with allies and within coalitions. Australia's use of non-US and UK based C3I systems require that considerable effort is placed in ensuring interoperability.

Interoperability is a multi-level concept that includes all level of war (tactical, operational and strategic) as well as interoperability with allies and coalitions. Interoperability does not mean the same in all cases. Full interoperability is not always required or desirable in these different cases. Different levels of interoperability would be used at national level as opposed to within a coalition. This is mostly due to security issues. Security is also the major implementation issue not only within Allies and Coalitions but also within Australian Systems.

To a large extend, interoperability in the Australia contact is still based on the passing of Formatted Messages, and has been for many years. No real advance has been made in this regard, mostly due to the problems caused by national security policy and practices. Recent initiatives, like, MIP Phase 2 and the Coalition Theater Logistics Advanced Concept Technology Demonstrator promise advancement to database replication and the use of information islands, but security is still an issue.

Interoperability will continue to be important issue in the future. The current state of interoperability of national systems is recognized as not being sufficient and work is underway under the JCSE initiative as well via industry participants. Interoperability with Australia's traditional allies will also be a continuing issue and resources and effort will be assigned to this task. Australia's continuing involvement is JWID is a good indication of this.

References

[ACT, 1995] The Center For Advanced Command Concepts and Technology (ACT) National Defense University, “Operations Other Than War (OOTW): The Technological Dimension”, NDU Press, 1995.

[Defence 2000], Defence 2000, Our Future Defence Force, Commonwealth of Australia 2000 ISBN 0 642 29544 1.

[ADFP 101] Australian Defence Force Publication 101.

[LISI, 1998] Levels of Information Systems Interoperability (LISI), US DOD C4ISR Architectural Working Group, March 1998.

[CITA, 1999], Combined Interoperability Technical Architecture (CITA) ACP 140 Version 1.0 3 May 1999.

[OS-OTG, 1999] Operational Specification for Over-The-Horizon Targeting Gold Revision C Change 2 OS-OTG (Rev C) (Ch 2), 1999.

[JTA, 2000], Department of Defense Joint Technical Architecture, Version 3.1, 31 March 2000.

[DIICOE, 2000] Defence Common Operating Environment (Defence COE) Rationale, Development and Use (R D & U) Document, 27 Sep 2000.

[C4ISR AWG, 1997] C4ISR Architectural Working Group, C4ISR Architecture Framework, Version 2.0, 1997.

[MPMP, 2002] Multilateral Interoperability Program Management Plan (MPMP), DRAFT Version B.0.

[CTL ACDT, 2001] Coalition Theater Logistics ACDT, Executive summary presentation, 2001, http://oak.man.external.lmco.com/ctl/public/ .

[JWID, 2002] Australian JWID 2nd Planning Session, Defence Knowledge Staff, 2002, http:// www.defence.gov.au/jwid/.

[AdatP3, 2001] Allied Data Publication 3, Baseline 10, 2001.

[US Army FM 100-5, 1993] U.S. Army's Field Manual 100-5, Operation, June 1993.

[CIX, 2002], JWID 2002 GCCS-COP Interoperability Implementation Guidelines, February 20, 2002.