9th International Command and Control Research and Technology Symposium

Coalition Transformation: An Evolution of People, Processes and Technology to Enhance Interoperability

C2 Interoperability – An Australian National Whole of Government Approach

Neil Warner
ADI Limited
59 Cameron Avenue
Belconnen Canberra ACT 2617
Australia
Neil.Warner@adi-limited.com
Phone: +61262565120
Fax: +61262565101

Abstract

Recent events in Australia's region of interest and around the world have shown that defence forces are increasingly being used to assist in a variety of civil crises and national emergencies. Such combined responses are throwing into relief the different procedures and command structures that often disparate organisations, even within the same sector of government, have evolved. These differences, which might range from the well established procedures within defence organisations staffed by highly trained professionals, to more loosely organised systems based largely on highly motivated civilian volunteers. With such a wide range of organisational cultures and resources it is clearly not practical to impose the same command and control procedures across all organisations, be they military or civil. A more productive and sensitive approach is to determine how to promote interoperability across this community in a way that is affordable and reasonably non- intrusive. Such imperatives for whole of government interoperability are not new to Australian strategic thought and have been discussed by government for the last 15 years.

Case studies are analysed that examine the level of interoperability that presently exists amongst organisations that cooperate to a large extent in the prevention, preparedness, response and recovery from incidents ranging from terrorism to bush fire fighting. These case studies are used to identify issues that need to be addressed and suggest ways in which these improvements might be realised. This is achieved by dividing the concept of interoperability into technical interoperability and organisational interoperability. This makes it easier to understand the issues that require attention. One of the major issues in whole of government interoperability is security and this is a complex area that does needs an innovative approach if it is not to inhibit effective interoperability.

Introduction

Defence forces are frequently required to work with other national organisations in responses to quite complex situations ranging from national emergencies to international operations often under United Nations' mandates. The result is a mixture of command and control cultures that are trying to establish common ground to achieve an effective outcome. For defence forces, in particular, this can represent a significant challenge in that highly structured defence organisations find themselves working with less well structured organisations. The only effective way forward is to develop procedures to allow useful and constructive interaction.

In response to this ever increasing trend in multi-organisational response to conflict and national emergency, governments need to be able to implement procedures that allow available civil and military resources to be marshalled and coordinated effectively. One means of initiating both an understanding of the issues involved as well as providing a solution is to develop a command support concept that can readily be integrated into the command and control hierarchy of each participating military organisation or civilian agency. The command support system proposed should provide an agreed and accepted interface through which information is passed and this includes sensitive information gathered by intelligence services operated by the participants. This can be quite a challenge in that, as will be addressed subsequently, each agency may have different guidelines by which it classifies sensitive information.

One means of stimulating a shared approach to command support would be to conduct civil defence planning and operations in close cooperation with defence forces through the established civil-military coordination processes. This would require that federal, state and local authorities cooperate to provide intelligence, local area supply and support and in so doing involve all these organisations in planning and the conduct of operations. To achieve this would require that a shared concept of command support resulting in some form of military and civil interoperability that would allow effective interfaces to be established between respective command and control systems.

In proposing this, however, due cognisance must be taken of the fact that military command and control systems are staffed by professional officers who spend a large percentage of their time in training and exercising to maintain a very high level of proficiency. By contrast, the majority of civil crisis management staff are mostly volunteers (especially in Australia), who have other careers and professions. Therefore, any shared concept of command support must also take into account the different levels of training and doctrine that will exist. Unless this can be accomplished, interoperability will not be achieved.

Aim

The aim is to examine the concept of interoperability as it applies to cooperation amongst a mixture of national organisations and agencies, and through this examination identify key issues that need to be understood and addressed.

Discussion of Interoperability

Introduction

Interoperability can be defined as the ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.[1]

In any discussion of interoperability, it is also necessary to examine the level of command to which interoperability procedures are to be applied. Various levels of command[2] exist in any military organisation. Within the Australian defence context, the following definitions are applicable.

- **Strategic** – responsible for coordinating the application of national power to achieve desired end state (National strategic and military strategic);
- **Operational** – concerned with the planning and conduct of campaigns to obtain military strategic objectives within a theatre of operations; and
- **Tactical -** commanders plan and conduct engagements to support operational level objectives.

Within these levels of command a degree of overlap exists because decisions at any particular level may affect many other levels within the command chain. Furthermore, higher-level commanders often need to resolve any tensions that arise between objectives at each level. Hence, the concept of interoperability must also be addressed within organisations and if this were more widely recognised, it would makes the transition to addressing and understanding interoperability amongst organisations much easier.

Interoperability can be partly, but not completely, subdivided into two distinct elements, namely, technical and organisational interoperability.

Technical Interoperability

Technical Interoperability can be defined as the ability of systems, to provide to and accept services from other systems and to use the services so exchanged to enable them to operate effectively together. A more formal definition has been proposed by the US DOD C4ISR Architectural Working Group and Combined Interoperability Technical Architecture (CITA) (ACP140)[3] from the CCEB using the Levels of

---

1 Australian Department of Defence (2000). Australian Defence Force Publication 101, Commonwealth of Australia.

2 Neil Warner, Trevor Finklaire, et al. (2001). Tactical Situation Awareness - A Multi-Layered Approach. Land Warfare Conference, Sydney, Defence Science and Technology Organisation.

3 Combined Communications and Electronics Board (2000). Combined Interoperability Technical Architecture (CITA) ACP 140 Version 1.0.

Information Systems Interoperability (LISI)[4]. Both these definitions lead to the conclusion that technical interoperability can be addressed through agreeing appropriate technical standards that allow technical interfaces to be determined and, if resources allow, addressed.

Organisational Interoperability

The concept of organisational interoperability was introduced by the Australian Defence Science and Technology Organisation (DSTO)[5] to cover the higher-level issues characterised by human-activity. Organisational interoperability stresses the organisational and cultural aspects rather than the technical, systems and operational aspects of interoperability. Organisational interoperability can consequently be much more difficult to address in that sensitivity needs to be applied in the interpretation of organisational culture and tradition and its relevance to developing a format for common purpose and action.

Four enabling attributes of organisation interoperability formed the basis of the model proposed by DSTO and the following evaluating questions were posed:

- **Preparedness:** What doctrine, experience and training enable the organisations to work together?
- **Understanding:** What level of information and knowledge sharing exists and how is the information used?
- **Command Style:** How are roles and responsibilities delegated or shared? and
- **Ethos:** What level of trust, culture, values and goals are shared?

This is The key issue within organisational interoperability is that it must include doctrine, people, procedures and training.

Imperatives for Interoperability

Introduction

The imperatives for whole of government interoperability are not new to Australian strategic thought, and is best stated from Australia's strategic planning in the 1990s and is stated below:

It is essential that we continue to improve our procedures for civil-military cooperation to provide intelligence, local area supply and support, and to match operational effectiveness with the needs of the civil community. It is important that the

---

4 US DOD C4ISR Architectural Working Group (1998). Levels of Information Systems Interoperability (LISI), US Department of Defense.

5 Thea Clark and Ross Jones (1999). "Organisational Interoperability Maturity Model for C2." Proceedings of the 1999 Command and Control Research and Technology Symposium.

ADF continue to involve federal, state and local authorities, as appropriate, in relevant operational planning and conduct of operations.[6]

This concept was further reinforced in the Defence Strategic Review 1993[7], which gives some guidance on civil-military coordination, and an extract from the key areas is shown below:

In time of conflict, the Government should be able to implement a unified national response in which available civil and military resources could be marshalled and effectively coordinated. …….…… It also calls for a civil-military interface in the theatre of operations, to coordinate implementation of our national response. Arrangements for coordinating Federal, State and Territory policy-making and advice need to be better defined and practised.

This can be summarised by the need to apply resources effectively to all stages of an incident, including:

- Prevention
- Preparedness
- Response
- Recovery

This is similar in concept to applying network centric warfare[8] (NCW) basics, including:

- Efficient sharing of information in real time;
- Common situation awareness of plans and operations; and
- Common view of commander's Intent.

Case Studies

To illustrate just how important an understanding of interoperability actually in initiating a cross organisational response several Australian case studies are considered using public domain information. It will be shown how the NCW constructs outlined above provide a means of understanding the issues involved in developing a concept of interoperability that leads to a command support system that can be used with different command and control systems for effective common purpose.

The context for both the management of the incidents considered and a whole of government approach has been derived from two Australian Department of Defence

---

6 Australian Department of Defence (1989). Australia's Strategic Planning in the 1990s, Australian Department of Defence.

7 Australian Department of Defence (1993). Australian Defence Strategic Review 1993, Australian Department of Defence,.

8 Alberts, D., J. Garstka, et al. (2002). Network Centric Warfare – Developing and Leveraging Information Superiority, CCRP.

Publications, namely Australia's Strategic Planning in the 1900s[9] and Australian Defence Strategic Review 1993[10]. Interoperability should be viewed from a global view, to enable a System of System approach as suggested by Krygiel in "Behind the Wizard's Curtain"[11]. However, this approach should not dictate the mission and goals of low-level tactical systems, these should be derived from the domain functions and required capabilities.

The type of incidents or situations that will be considered are:

- Natural Disasters;
- Operations Other Than War
- Coastwatch including anti people smuggling operations; and
- Counter Terrorism.

The primary missions and goals are:

- To provide intelligence, local area supply and support to both civilian and military authorities;
- For the government to involve federal, state and local authorities, as appropriate, in relevant operational planning and conduct of operations;
- That both civil and military resources could be marshalled and effectively coordinated to achieve appropriate goals and outcomes; and
- The coordination of civil and military interests at the Ministerial level, and close consultation among senior policy advisers

Derived secondary goals appear to be:

- Calls for a civil-military interface in the theatre of operations, to coordinate implementation of an Australian national response; and
- Civil defence planning and operations should be conducted in close cooperation through the established coordination processes, which should be exercised regularly.

Canberra Fires of 2002[12]

Bushfires in Australian are a seasonal hazard and great efforts are placed in the prevention, preparedness, response and recovery from bushfire incidents.

---

9 Australian Department of Defence (1989). Australia's Strategic Planning in the 1990s, Australian Department of Defence.

10 Australian Department of Defence (1993). Australian Defence Strategic Review 1993, Australian Department of Defence,.

11 Annette J Krygiel (1999). Behind the Wizard's Curtain - An Integrated Environment for a Systems of Systems, National Defense University and the US DOD CCRP.

12 Ron McLeod (2003). Inquiry into the Operational Response to the January 2003 Bushfires in the ACT. Canberra, ACT Government.

On Saturday 18 January 2003 the bushfires, which had been burning in the hills to the west and southwest of Canberra for more than a week, reached the perimeter of the city. The result was widespread damage to rural properties, parks and forests, more than five hundred houses were destroyed along with significant urban infrastructure, estimated at approximately $300 million. Tragically, four people died. Drought and weather were major factors in the spread of the fire.

Those involved subsequently in the operation included:

- Australian Capital Territory (ACT) Emergency Service Bureau, including the ACT Fire Service, ACT Ambulance Service and ACT Bushfire Service;
- Australian Federal Police, who provide policing for the ACT;
- New South Wales (NSW) Rural Fire Service;
- Victoria Country Fire Authority (CFA);
- Emergency Management Australia, in the coordination of assistance from interstate and federal agencies;
- Department of Defence (DOD), providing heavy equipment, manpower and Aircraft; ; and
- Many other Government Departments and Non Government Aid Agencies

The majority of emergency services in Australia depend on radio communications, mostly in the VHF band. Telephones and mobile phones are used at, from, and to headquarters. The ACT Emergency Services Branch (ESB) concluded, "Radio communications systems did not meet the substantial demands created by an event of this magnitude"[13]. Among the problems brought to the Inquiry's attention were the following:

- Inadequate coverage;
- Congestion on various networks;
- Overwhelming of the communication centre;
- Apparent shielding, possibly because of dense smoke;
- Inadequate ground–air communication;
- Difficulties with interoperability between the various firefighting elements; and
- Insufficient quantities of equipment.

It was further noted by all, and especially commented on in the McLeod Inquiry[14], that apart from the ACT Emergency Services, all other participants used communications equipment of different types that were incompatible. It was noted that the different communications procedures followed by emergency service bodies across Australia and the DOD are related to decisions taken by the separate jurisdictions at different times, seeking to take best advantage of rapidly changing technology. Further, although the aircraft could communicate with one another, due to the requirements of airspace control, it was a rare occurrence when an aircraft could directly communicate with ground units, either to report the fire fronts or to provide directions to water bombing aircraft.

---

13 Ibid.

14 Ibid.

Although the operation was directed from the ACT ESB Operations Centre, the other operations centres involved (Defence, NSW RFS and Victorian CFA) did not have easy and simple procedures and technology for interaction. Problems within the command and control relationship between the ACT Fire Brigade and ESB appeared to exist as well as differences in the command and control philosophies of the ACT and New South Wales bushfire services. It was perceived that the Incident Control System[15] (ICS) arrangements in New South Wales are more aligned to the national approach. By contrast, ACT bushfire brigade captains have greater operational independence and responsibility.

From an examination of the responses mounted to the Canberra fires, it can be concluded that problems with interoperability existed at both the technical and operational level. On the technical level radios and information systems were for the most part incompatible. Organisational interoperability was actually non existent.

Regional Assistance Mission to the Solomon Islands[16]

Over the period from 1998 to 2003, ethnic tension and violence caused the deterioration of the rule of law in the Solomon Islands until most aspects of government, including hospital, schools and policing ceased to exist. The Solomon Islands had descended to an inflammable mixture of guns, ethnic tensions, rogue police, corrupt politicians and business people, and armed criminals.

The Government of the Solomon Islands' loss of control was widely acknowledged across the community and a request for external intervention was subsequently sanctioned by a unanimous vote of the Solomon Islands Parliament.
The Regional Assistance Mission to Solomon Islands, or RAMSI as it is widely known, was subsequently created to provide a solution. Under RAMSI[17], the deployment of about 300 police officers, backed by 1700 military personnel, from nine regional countries (Australia, New Zealand, Fiji, PNG, Tonga, Samoa, Vanuatu, Kiribati, and Cook Islands) was undertaken to stabilise the situation. RAMSI in the first vital phase, which is what is considered here, was a police led operation, with the military playing a support role, providing protection and logistical assistance, but also helping to build a crucial environment of civil compliance. The task of the police was to establish immediately law and order in Honiara, working closely with the Royal Solomon Island Police.

---

15 The Incident Control System is used for managing emergency situations using a systematic approach, which effectively copes with all the activities, which occur at an incident. The type and scale of the incident does not affect the principles of the system and can be used in a wide range of situations, bushfires, floods and earthquakes are examples. The ICS has been modified to suit Australian needs from the original idea developed in America, where it was developed by adapting military command and control principles. Since the late 1980's, throughout Australia, the majority of emergency services and fire-fighting agencies have adopted the ICS as their method for incident management. Jennifer Bean (2002). "The Implementation of the Incident Control System in NSW: Span of Control and Management by Objectives." AUSTRALIAN JOURNAL OF EMERGENCY MANAGEMENT **Volume 17**.

16 Mr Nick Warner (2003). Operation Helpem Fren: Rebuilding the Nation of Solomon Islands.

17 Australian Department of Defence (2004). Operation Anode - Regional Assistance Missions to the Solomon Islands, Australian Department of Defence,. **2004**.

The Australian contribution to the multinational stabilisation force comprised about 1,500 Australian Defence Force personnel, 155 Australian Federal Police and 90 personnel from the Australian Protective Service. Military personnel from Australia, Fiji, Tonga, New Zealand and Papua New Guinea provided security for police assisting the Solomon Islands Government.

Tactical communications presented a problem between civilian elements (AFP and APS) and Australia Army and Naval units. Tactical Communications between all participating military units also created a problem[18]. The initial use of the LPA HMAS Manoora, which has command ship capabilities, provided operational communications back to the Australian Headquarters and established a ready made operational and tactical command post.

- Technical interoperability from tactical to operational level did not exist or was very poor. There also appeared to be a lack of organisational interoperability.

This operation was planned and executed quite rapidly, but there did not appear to be any mechanism to alleviate the problems of organisational and technical interoperability. The success in quickly re-establishing rule of law through the widespread placement of enforcement personnel under the umbrella of RAMSI indicates that shortcomings in technical interoperability were overcome reasonably well in a short time. However, interoperability at the operational level appears not to have been addressed.

Pong Su Incident

On 23 April 2003, Australian Police observed the Tuvala registered, North Korean owned, freighter Pong Su close to shore and followed two Chinese suspects on the shore as they left the beach and headed for a near-by hotel. The next morning, the two suspects were apprehended at their hotel with 50 kgs of pure heroin. In a subsequent search of the beach, where the two suspects had been seen the day before, Australian police discovered the body of a North Korean recently buried close to a dingy. It is probable that the dingy had capsized while bringing the heroin ashore, drowning one of the North Koreans. Police also apprehended another North Korean in the immediate area. Unable to get back to his boat, he had simply remained in the area where the drugs had been landed the night before.

The Pong Su led Australian police vessels on a four-day chase in 30-foot swells until commandos boarded the freighter by helicopter and boat. Australian authorities ordered the Pong Su into harbour, but the ship attempted to escape into international waters. After a helicopter boarding by the Australian Defence Forces SASR, the Pong Su was brought into port. Australia's Incident Response Regiment was also deployed, indicating Australia's suspicion that weapons of mass destruction might be on board.

[18] It was reported that composite units were created, that utilize Australian Tactical Communications equipment, therefore overcoming the tactical communication problems.

The ethnic Chinese suspects and the captain and crew of the Pong Su have been charged with narcotics trafficking. The 29 remaining crewmembers, also North Koreans, were arrested and charged with aiding and abetting narcotics smuggling.

Initial detection was made by both the Victoria Police and the Australian Federal Police. The Coastwatch (part of Customs) and the Royal Australian Navy conducted tracking of the vessel up the Australian Coast (see Figure 3). Seizure of the vessel was a joint operation between the RAN, SASR and Australian Federal Police.

The Australian Defence Force's special operations commander, Major General Duncan Lewis[19], says heavily armed officers seized the Pong Su in very high seas. The SASR quickly boarded the vessel and then sought to dominate by securing the bridge. The vessel was brought under our control in a matter of minutes really from the time the boarding commenced and as soon as the ship was declared secure, then very clearly, in accordance with the regulations, we handed jurisdiction back to the Customs and Australian Federal Police officers."

Figure 1[20] – PONG SU Incident – MAP OF PURSUIT

The agencies involved with this operation were:

- Victoria Police, using internal information systems;
- Australian Federal Police; using PROMIS[21]; and

---

19 ABC News Online (2003). Crew held after daring drug raid at sea, ABC News Online. **2004**.

20 Australian Department of Defence (2003). Pursuit of PONG SU, Australian Department of Defence.

21 Police Real Time Online Management System (PROMIS). PROMIS provides the AFP with a single, consistent system for documenting the progress of investigations, information collection and its subsequent retrieval. It also provides an improved capacity to nationally

- Department of Defence, especially Special Forces using a combination of the Joint Command Support System[22] (JCSS) and the Special Operations Command Support System[23] (SOCSS).

None of these organizations shares a common information system at the classified level nor has any systems interconnect to provide the transmission of classified information.

The operations surrounding the seizure of the Pong Su were seen as an unprecedented success. It was an operation dominated mostly by technical interoperability in that a well defined task was presented to all participants. However, further improvements in technical interoperability might have been achieved if the appropriate information systems had been more widely used.

Counter Terrorism[24] Exercises in Australia

Following the Hilton Hotel Bombing in Sydney in 1978, the then-Prime Minister, Malcolm Fraser, announced the establishment of a committee which would include Commonwealth and State Agencies, principal aim of which would be to establish a set of national arrangements and agreements to respond to threats or acts of politically motivated violence. The Standing Advisory Committee on Commonwealth/State Cooperation for Protection Against Violence (SAC-PAV) held its first meeting in February 1979[25].

Counter Terrorism exercises are part of the Australian Government approach to emphasise the importance of being prepared for such incidents and demonstrate high-

---

manage operations and facilitates consistency in the way in which operations are undertaken across the whole organisation. Australian Federal Police (2004). AFP Newsletter, Australian Federal Police. **2004**.

22 JCSS is an integrated command, management and communications System supporting the command and control of ADF operations. Whereas JCSS is focused on joint operations and the strategic and operational levels of command, ACSS is primarily intended to support the command and control (C2) of air operations at the operational and tactical levels. Australian Department of Defence (2004). Joint Command Support System, Defence Material Organisation. **2004**.

23 SOCSS allows special operations commanders to understand situations rapidly, formulate strategies, preview operations and execute missions. The system ultimately provides commanders with the intelligence and visibility necessary to control resources in dynamic situations. ADI Limited (2004). Special Operations Command Support System, ADI Limited. **2004**.

24 A 'terrorist act' is an act or threat, intended to advance a political, ideological or religious cause by coercing or intimidating an Australian or foreign government or the public, by causing serious harm to people or property, creating a serious risk of health and safety to the public, disrupting trade, critical infrastructure or electronic systems. Counter-terrorism will include the full range of activities covering prevention, preparedness, detection, response and recovery. Threats to Australian people, property and interests, including critical infrastructure, will be considered.

25 Australian Attorney-General's Department (2004). Protecting Australia, Commonwealth of Australia. **2004**.

level commitment from Federal and State and Territory counter-terrorism agencies with a role in security, law enforcement, intelligence and emergency management[26].

In 2004, the Mercury 04 series of exercises, that are a five-day exercises, are part of the Government's 2003 Budget commitment of $15.7 million over four years to broaden the number and scope of counter-terrorism exercises. The first of five counter-terrorism exercises in 2004, Mercury 04 will test arrangements in four jurisdictions - the Northern Territory, Tasmania, South Australia and Victoria - and Australian Government agencies. A range of complex terrorism scenarios will be managed, which will provide an opportunity for some of the jurisdictions to test new chemical, biological and radiological (CBR) equipment and critical infrastructure protection[27].

The organisation of counter terrorism forces for Australia is detailed within the National Counter-Terrorism Plan[28] published by the National Counter Terrorism Committee[29]. The basic organisation is shown in Figure 2 below. Organisation at an incident (exercise or operation) is shown in Figure 3. The important aspect of this is that the Police remain in control and not the contingent from Defence once the SASR Tag is called out.

---

26 Australian Attorney-General's Department (2004). A Safer Australia, Commonwealth of Australia. **2004**.

27 Ibid.

28 National Counter-Terrorism Committee (2003). National Counter-Terrorism Plan, Commonwealth of Australia.

29 National Counter-Terrorism Committee is co-chaired by PM&C and a State/Territory senior official and comprises senior representation from relevant Commonwealth agencies, Premiers' and Chief Ministers' departments and police services from each jurisdiction. Ibid.

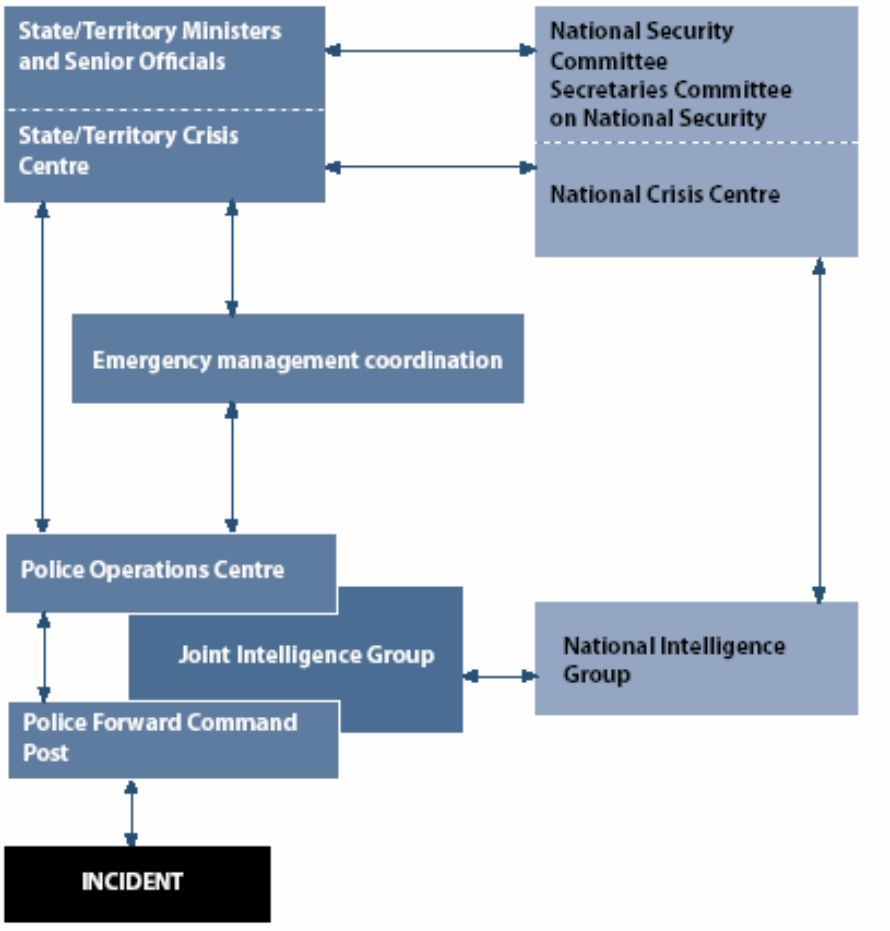

Figure 2[30] – COUNTER-TERRORISM MANAGEMENT ARRANGEMENTS

As shown in the Figure 2 and the discussion with respect to the Mercury 04 Exercises, the following agencies could be involved in counter terrorism exercises or operations. Their information systems are also briefly discussed.

- Protective Security Coordination Centre (Attorney-Generals Department (AGs), use an internal AG Information System and would have access to ASNET;
- Australia Federal Police – use the PROMIS System, previously discussed, and would have access to ASNET;
- Emergency Management Australia – Consequent Management, use an internal AGs Information System;
- State Police Forces include Tactical Response Groups and Crisis Management Centres. Use an internal Information Systems that differ from state to state;
- Department of Defence, especially Headquarters Special Forces, Defence Intelligence Organisation, the Special Air Service Regiment, 4th Battalion the Royal Australian Regiment (Commando), Tactical Assault Groups (West) and (East), 1st Commando Regiment and the Incident Response Regiment under

30 Ibid.

the Defence Legislation Amendment (Aid to Civilian Authorities) Act 2000[31]. DOD uses a combination of Joint Intelligence Support System (JISS), JCSS and SOCSS and would have access to ASNET.

- Australian Security Intelligence Organisation for Intelligence
- Many other Commonwealth and State agencies for Consequence Management

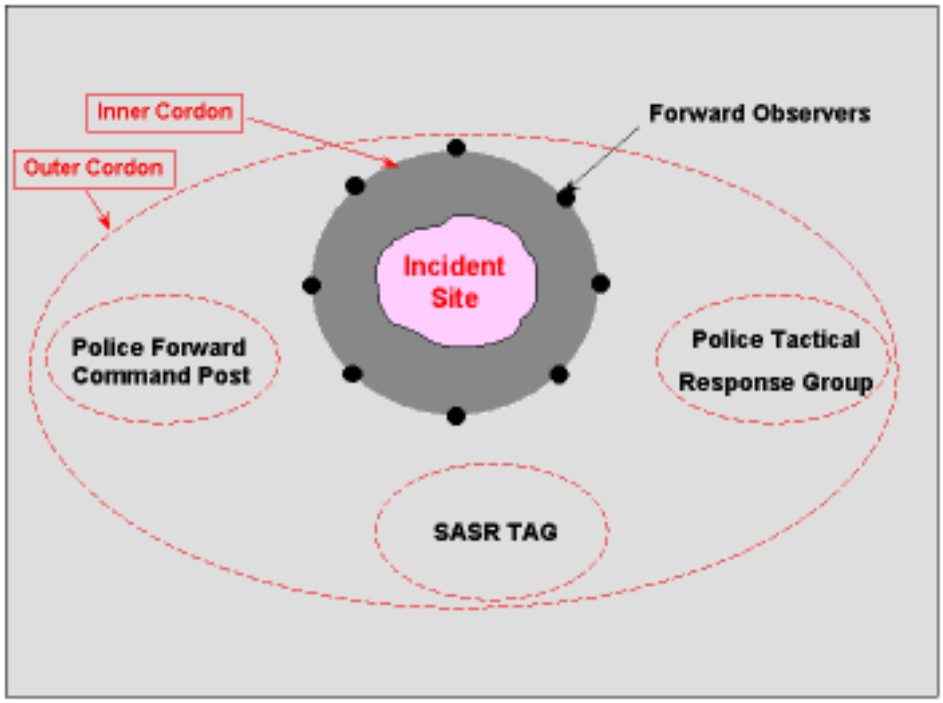

Figure 3[32] – COUNTER TERRORISM INCIDENT GEOGRAPHIC ORGANISATION

It is evident that, a large degree of organisational interoperability exists and this is clearly detailed in the National Counter Terrorism Plan. Technical interoperability, however, appears to be less well served, with only ASNET providing some level of information exchange, probably at the strategic and operational level for intelligence. It is unclear whether tactical intelligence could flow in the time scale required over ASNET or whether any operational data would flow over ASNET.

---

31 Australian Attorney-Generals Department (2000). DEFENCE LEGISLATION AMENDMENT (AID TO CIVILIAN AUTHORITIES) ACT 2000 No. 119, 2000, Commonwealth of Australia. **2004**.

32 SGT Bob Wynn (2004). AFP Counter Terrorism Procedures. N. Warner. Canberra.

Technical Interoperability

From and examination of the above case studies, the greatest deficiency in achieving technical interoperability is the lack of interoperability of tactical communications systems, especially radio networks. Every organisation uses a different radio network type based on its own unique requirements, which, as far as can be determined, take little or no account of interoperability between organisations. Something as relatively simple as of common waveform types across the radio networks does not appear to have been considered.

The greatest impact would be achieved through the establishment of a high capacity tactical radio network across all levels of government that could provide for communications between all parties as and when required. This radio network should be capable of transmitting both voice and data and be based on digital technology to take advantages of technologies that reduce bandwidth demand as well as allowing information to be encoded identifying network users automatically. This network would not be easy to establish in Australia as a fixed installation due to the vast distances involved, but there is technology being developed that could allow ad hoc networks to be established as gap fillers with links into the fixed infrastructure. A more immediate option is the use of digital switches and gateways to join radio networks and PSTN systems together.[33] Nevertheless, the concept of a shared tactical radio network remains a robust objective in achieving technical interoperability.

Technical Interoperability does, however, exist at the operational and strategic level to some degree through the use of fixed, unclassified IT Systems. Common use of the LISI Model at Level One allows message passing to be achieved between different organisations. However, this not the case across classified systems due to the differing security levels and security level systems that are used by the Australian Federal Government and State Governments, which is indicative of the very low level of organisational interoperability.

Organisational Interoperability

The case studies show that organisation interoperability could only be established if there were some basis for common organisation, procedures and actions amongst organisations. It is, therefore, suggested that the Incident Control System (ICS) be implemented as the basis for obtaining organisation interoperability at the tactical and operational level. Since the ICS was developed from defence command and control principles, it is thought that this could be quickly adopted, with modification, and would minimise political problems as well as organisational inertia.

---

[33] CISCO Systems demonstrated at the DSTO Land Warfare Conference 2004 an IP Radio Gateway that provides connectivity between UHF, VHF Military Radios, and Voice over IP and PSTN Systems. Andre Obradovic (2004). Cisco Systems Transforming Defence Communications. Land Warfare Conference 2004, CISCO Systems.

The principles applied to the planning and conduct of operations also appear to be different across organisations with similar purposes both at state and federal level. Once again, this generally indicates a low level of organisational interoperability.

To improve organisational interoperability, efforts should be made throughout government, both state and federal levels, to establish a common security classification system. This would at least allow for interoperability between systems sharing information at the same level.

Key Issue of Security

A key issue that emerges from the case studies is that of security. It is also an issue in which both technical and organisational interoperability must be addressed in concert if widely accepted solutions are to be achieved. New principles are established and agreed to allow the exchange of classified information.

The problems faced due to security can be illustrated by considering the different designations used for security levels by Australian federal agencies:

- Defence
  - Unclassified
  - Restricted
  - Confidential
  - Secret
- Attorney-Generals
  - Unclassified
  - Protected
  - High protected

This is not an issue that will be easily overcome. The requirement for "need to know" in all jurisdictions works against the "all informed" concept with most information systems. Hence we are confronted by the operational interoperability issues associated with the principle of "need to know" and the technical interoperability of information systems designed to provide wide seamless access. These contradictions restrict the extent to which interoperability can be achieved.

From a technical interoperability perspective, the advent of multi level secure systems should be able to eliminate, at least to some extent, this problem. In addition, the introduction and use of trusted data diodes and transfer mechanisms would be another advance. However, these technologies have been discussed for some years and they have yet to be widely implemented.

Operational interoperability could be addressed through the implementation of a security architecture. Such a security architecture needs to be segmented into at least four security domains (as shown in Figure 4) to protect information correctly within the system. This also allows for existing infrastructure within Defence, Attorney-Generals, Emergency Management Australia, AFP, Coastwatch and other Federal Government Departments to be utilised. At least four domains would be required, as discussed below:

TOP SECRET Domain – Defence based for the sharing of intelligence information, with PSCC and AFP and other appropriate organisation gaining access. This could be based on the current ASNET.

SECRET Domain – Defence based on the current JCSS. JCSS has an IP based Intranet type system. Its precise configuration is classified and will not be detailed within this design. Civil agencies like PSCC could also share this domain as Coastwatch's National Surveillance Centre (NSC) current resides on the JCSS. This domain would be primarily focused on the "Defence or Australia" and other similarly functions including Defence, Counter Terrorism, OOTW and asymmetric warfare.

PROTECTED Domain – Other government organisations maintained based on the extension to the current Coastwatch Network but could incorporate the AG's and AFP. The Coastwatch network is an extension of the Customs Service WAN and runs medium level encryption to protect the information. This domain would be focused on coastal and air space surveillance. Intelligence reports could be injected at this level, depending on their origin.

UNCLASSIFIED Domain - Maintained by Emergency Management Australia (should this be open to all sources) providing links to all state and local based organisations that would require or could input the information. This domain would also include AMSA[34]. This domain of the system would be based on the Internet and could use low level encryption if required (This requirement would need to be further examined). This domain would concentrate on emergency management and civil Defence. Open or Public intelligence reports could also be inputted at this level. Air traffic control position reports and coastal shipping information could be injected at this level. Local Government Authorities, NGOs and other similar organisations would need to interact with the system at this security domain.

---

[34] The Australian Maritime Safety Authority is a largely self-funded government agency with the charter of enhancing efficiency in the delivery of safety and other services to the Australian maritime industry. AMSA will pursue world's best practice in the efficient provision of highly effective maritime safety, aviation and marine search and rescue, and marine environment protection services. Australian Maritime Safety Authority (2004). AMSA Web Page, Commonwealth of Australia. **2004**.

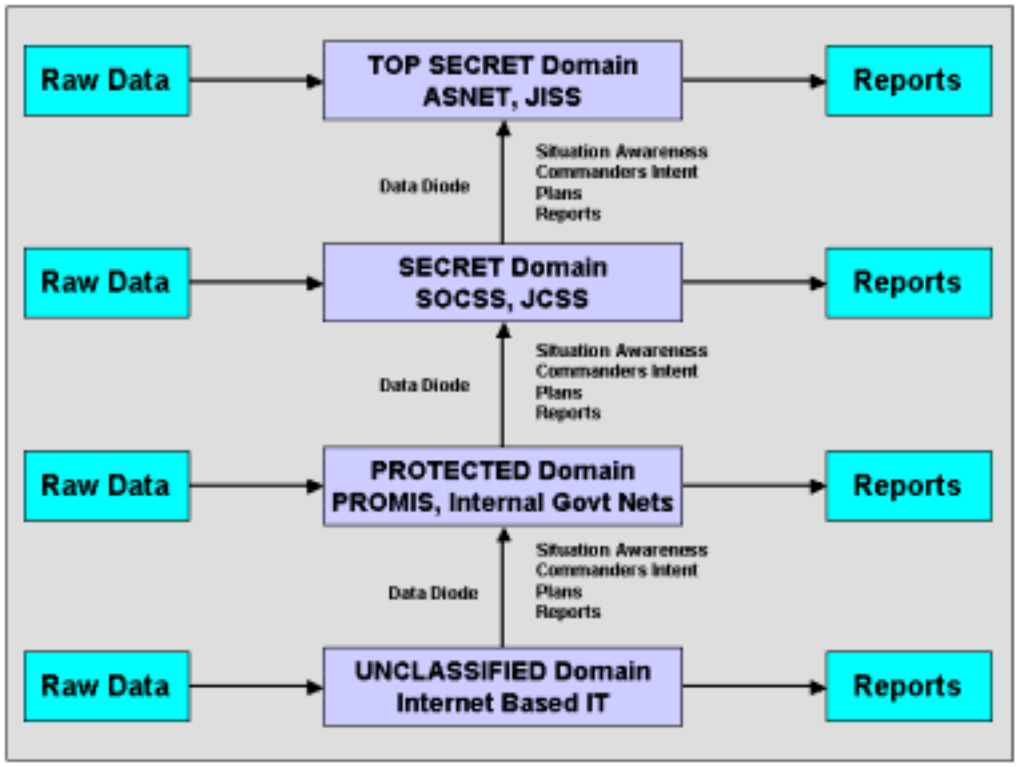

Figure 4 – Overview of Security Architecture

Conclusion

Interoperability can be broadly subdivided into two distinct elements technical and organisational interoperability. Both technical and organisational interoperability issues must be solved for true interoperability to exist.

Technical interoperability requirements are easier to define and are also easier to achieve in incidents that have relatively few objectives, even when a number of agencies are involved.

Operational interoperability, because it embodies the established operating procedure of each organisation cannot be achieved during an incident, it must be addressed and solved prior to any operation involving multiple agencies

Case studies have shown the within the Australian context, that whole of government interoperability does not yet exist for either organisational or technical interoperability.

Whole of Government interoperability remains a national imperative.
The Incident Control System could be implemented as the basis for obtaining organisation interoperability at the tactical and operational level.

A major inhibitor for attaining technical interoperability is the lack of a tactical radio network operating across all levels of government.

.

A key issue in achieving whole of government interoperability is security.

Technical interoperability issues in regard to security can be easily solved; however, organisational interoperability will require significant effort and the development of a security architecture for this purpose is proposed.

References

ABC News Online (2003). Crew held after daring drug raid at sea, ABC News Online. **2004**.

ADI Limited (2004). Special Operations Command Support System, ADI Limited. **2004**.

Aerosonde Limited (2004). Aerosonde deploying to The Solomons in Support of Australian Troops, Aerosonde Limited. **2004**.

Alberts, D., J. Garstka, et al. (2002). Network Centric Warfare – Developing and Leveraging Information Superiority, CCRP.

Andre Obradovic (2004). Cisco Systems Transforming Defence Communications. Land Warfare Conference 2004, CISCO Systems.

Annette J Krygiel (1999). Behind the Wizard's Curtain - An Integrated Environment for a Systems of Systems, National Defense University and the US DOD CCRP.

Australian Attorney-Generals Department (2000). DEFENCE LEGISLATION AMENDMENT (AID TO CIVILIAN AUTHORITIES) ACT 2000 No. 119, 2000, Commonwealth of Australia. **2004**.

Australian Attorney-General's Department (2004). Protecting Australia, Commonwealth of Australia. **2004**.

Australian Attorney-General's Department (2004). A Safer Australia, Commonwealth of Australia. **2004**.

Australian Department of Defence (1989). Australia's Strategic Planning in the 1990s, Australian Department of Defence.

Australian Department of Defence (1993). Australian Defence Strategic Review 1993, Australian Department of Defence,.

Australian Department of Defence (2000). Australian Defence Force Publication 101, Commonwealth of Australia.

Australian Department of Defence (2000). Defence 2000, Our Future Defence Force, Commonwealth of Australia 2000, Commonwealth of Australia.

Australian Department of Defence (2003). Pursuit of PONG SU, Australian Department of Defence.

Australian Department of Defence (2004). Joint Command Support System, Defence Material Organisation. **2004**.

Australian Department of Defence (2004). Operation Anode - Regional Assistance Missions to the Solomon Islands, Australian Department of Defence,. **2004**.

Australian Federal Police (2004). AFP Newsletter, Australian Federal Police. **2004**.

Australian Maritime Safety Authority (2004). AMSA Web Page, Commonwealth of Australia. **2004**.

Combined Communications and Electronics Board (2000). Combined Interoperability Technical Architecture (CITA) ACP 140 Version 1.0.

Jennifer Bean (2002). "The Implementation of the Incident Control System in NSW: Span of Control and Management by Objectives." AUSTRALIAN JOURNAL OF EMERGENCY MANAGEMENT **Volume 17**.

Mr Nick Warner (2003). Operation Helpem Fren: Rebuilding the Nation of Solomon Islands.

National Counter-Terrorism Committee (2003). National Counter-Terrorism Plan, Commonwealth of Australia.

Neil Warner, Trevor Finklaire, et al. (2001). Tactical Situation Awareness - A Multi-Layered Approach. Land Warfare Conference, Sydney, Defence Science and Technology Organisation.

Nick Warner (2004). Operation Helpem Fren: Rebuilding the Nation of Solomon Islands, Australian Department of Foreign Affairs and Trade. **2004**.

Ron McLeod (2003). Inquiry into the Operational Response to the January 2003 Bushfires in the ACT. Canberra, ACT Government.

SGT Bob Wynn (2004). AFP Counter Terrorism Procedures. N. Warner. Canberra.

Thea Clark and Ross Jones (1999). "Organisational Interoperability Maturity Model for C2." Proceedings of the 1999 Command and Control Research and Technology Symposium.

United States Army (1993). US Army Field Manual 100-5, US Army.

US DOD C4ISR Architectural Working Group (1998). Levels of Information Systems Interoperability (LISI), US Department of Defense.