



Air Power Development Centre

**NETWORK CENTRIC WARFARE  
AND THE  
FUTURE OF AIR POWER**

**THE PROCEEDINGS OF A CONFERENCE  
HELD IN CANBERRA BY  
THE ROYAL AUSTRALIAN AIR FORCE**

**16–17 SEPTEMBER 2004**

**Edited by Wing Commander Keith Brent, CSC**

© Commonwealth of Australia 2005

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission. Inquiries should be made to the publisher. The papers written by Air Vice-Marshal Iain McNicoll, *Network Centric Warfare – Perspectives from the United Kingdom*, and Group Captain Chris Finn, *Network Centric Warfare – Doctrinal Issues*, also are subject to Crown copyright protection.

### **Disclaimer**

The views expressed are those of the authors and conference participants, and do not necessarily reflect the official policy or position of the Department of Defence, the Royal Australian Air Force or the Government of Australia, or the official policy or position of the respective Armed Forces or Governments of the overseas participants. The Commonwealth of Australia will not be legally responsible in contract, tort or otherwise, for any statements made in this record of proceedings.

### **Release**

This document is approved for public release. Portions of this document may be quoted or reproduced without permission, provided a standard source credit is included.

---

National Library of Australia  
Cataloguing-in-Publication entry

Network Centric Warfare and the Future of Air Power (2004 : Canberra, A.C.T.).

Network centric warfare and the future of air power : the proceedings of a conference held in Canberra by the Royal Australian Air Force, 16–17 September 2004.

ISBN 0 642 26599 2

1. Air power - Australia - Congresses. 2. Command and control systems - Australia - Congresses. 3. Military art and science - Australia - Congresses. I. Brent, Keith, 1944- . II. Australia. Royal Australian Air Force. Air Power Development Centre. III. Title.

358.400994

---

Published and distributed by:

Air Power Development Centre  
Level 3  
205 Anketell Street  
TUGGERANONG ACT 2900  
AUSTRALIA

Telephone: + 61 2 6266 1355  
Facsimile: + 61 2 6266 1041  
E-mail: [airpower@defence.gov.au](mailto:airpower@defence.gov.au)

# CONTENTS

<b>Preface and Acknowledgments</b>	v
<b>Notes on Contributors</b>	vii
<b>Abbreviations</b>	xxi
<b>WELCOME ADDRESS</b> Air Marshal Angus Houston, AO, AFC	1
<b>OPENING ADDRESS:</b> <b>NETWORK CENTRIC WARFARE – THE ADF ROADMAP</b> Senator the Honourable Robert Hill, BA, LLB, LLM, FTIA	3
<b>KEYNOTE ADDRESS:</b> <b>THE FUTURE OF AIR POWER – RAAF RESPONSE TO THE ADF ROADMAP</b> Air Marshal Angus Houston, AO, AFC	9
<b>NETWORK CENTRIC WARFARE AND AIR POWER</b> Lieutenant General Joseph E. Hurd (USAF, Retired)	23
<b>NETWORK CENTRIC WARFARE – PERSPECTIVES FROM THE UNITED KINGDOM</b> Air Vice-Marshal Iain McNicoll, CBE, BSc, FRAeS, RAF	37
<b>INTERNATIONAL PANEL:</b> <b>THE VALUE OF NETWORK CENTRIC WARFARE TO AIR POWER</b> Air Marshal Subhash Bhojwani (Indian Air Force) Lieutenant General Dato' Azizan bin Ariffin (Royal Malaysian Air Force)	51
<b>NETWORK CENTRIC WARFARE AND THE ADF – CRITICISMS AND POTENTIAL PITFALLS</b> Professor Ross Babbage	67
<b>SEVEN PROPOSITIONS ABOUT CLOSE AIR ATTACK ON THE FUTURE BATTLEFIELD</b> Dr Alan Vick	83

<b>SAY AGAIN? – A (VERY) BRIEF HISTORY OF NETWORK CENTRIC WARFARE</b>	95
Dr Alan Stephens	
<b>FUTURE OPTIONS FOR AUSTRALIAN AIR POWER</b>	103
Mr Sanu Kainikara	
<b>NETWORK CENTRIC OPERATIONS AND MODULAR SYSTEMS</b>	117
Lieutenant General Carl O’Berry (USAF, Retired)	
<b>NETWORK CENTRIC WARFARE – DOCTRINAL ISSUES</b>	137
Group Captain Chris Finn, RAF	
<b>INFORMATION MANAGEMENT – THE KEY TO NETWORK CENTRIC WARFARE</b>	151
Air Vice-Marshal Julie Hammer, AM, CSC	
<b>THE FUTURE OF THE NAVY AND NETWORK CENTRIC WARFARE</b>	171
Vice Admiral Chris Ritchie, AO, RAN	
<b>THE FUTURE OF THE ARMY AND NETWORK CENTRIC WARFARE</b>	183
Lieutenant General Peter Leahy, AO	
<b>NETWORK CENTRIC WARFARE AND RAAF PEOPLE – VIGNETTES OF THE FUTURE</b>	197
Squadron Leader Tim Anderson	
Squadron Leader Cheryl Neal	
Squadron Leader Dominic Sims	
<b>OBSERVATIONS ON THE CONFERENCE</b>	211
Air Vice-Marshal Roxley McLennan, AM	
<b>CLOSURE</b>	215
Air Marshal Angus Houston, AO, AFC	

## **PREFACE AND ACKNOWLEDGMENTS**

Papers have been printed as provided by the authors, with only minor changes to achieve some consistency in layout, spelling and terminology. The transcripts of the panel discussions that followed the presentation of the papers have been edited for relevance, clarity and brevity. Copies of the edited papers and transcripts were sent to the authors for clearance before publication.

My thanks are due to my colleagues at the Air Power Development Centre, in particular Miss Michelle Lovi, for their highly professional editorial assistance.

Keith Brent  
Air Power Development Centre  
Canberra

June 2005



## **NOTES ON CONTRIBUTORS**

### **AIR MARSHAL ANGUS HOUSTON, AO, AFC**

Air Marshal Houston joined the Royal Australian Air Force (RAAF) as a cadet pilot in 1970 and spent the early part of his career flying Iroquois helicopters in various parts of Australia, Papua New Guinea and Indonesia. After graduation from Flying Instructors Course in 1975, Air Marshal Houston completed several instructional tours on Macchi, BAC Strikemaster and Iroquois aircraft. A posting to the Republic of Singapore Air Force (RSAF) from 1976 to 1978 was followed by two years at No 9 Squadron at RAAF Base Amberley. In late 1979 Air Marshal Houston was posted to Hill Air Force Base, Utah, for exchange flying duties with a United States Air Force (USAF) helicopter unit. In 1980, he was awarded the Air Force Cross (AFC) for an open sea rescue in gale force winds the previous year.

After a further posting to No 9 Squadron as the Executive Officer, and staff training at RAAF Staff College, Air Marshal Houston was posted to the Department of Air (Development Division) where he was involved in the Black Hawk Helicopter Project. In 1987, Air Marshal Houston assumed command of No 9 Squadron in time for the introduction of the Black Hawk, relocation of the unit from Amberley to Townsville, and its transfer to the Australian Army. In 1989, he enjoyed one year as a Squadron Commander with the 5th Aviation Regiment. Air Marshal Houston was admitted as a Member in the Military Division of the Order of Australia (AM) in 1990 for his work in the transfer of responsibility for Black Hawk operations.

Following graduation from Joint Services Staff College, Air Marshal Houston was posted to the Joint Operations staff at Headquarters Australian Defence Force and was involved in strategic planning during the Gulf crisis of 1990/91. On promotion to Group Captain in July 1992, he assumed the post of Director Air Force Policy and negotiated the establishment of the RSAF Flying School at RAAF Base Pearce. After completing a C-130H conversion in 1993, Air Marshal Houston commanded No 86 Wing from 1994 to 1995.

Air Marshal Houston attended the Royal College of Defence Studies in London in 1996. He was Chief of Staff, Headquarters Australian Theatre from 1997 to 1999, Commander Integrated Air Defence System from 1999 to 2000, and Head Strategic Command from August 2000. Air Marshal Houston was appointed as Chief of Air Force on 20 June 2001. He was promoted to Officer of the Order of Australia (AO) in the 2003 Australia Day Honours List.

Air Marshal Houston is married to Liz, who is a teacher, and they have three sons.

### **SENATOR THE HONOURABLE ROBERT HILL, BA, LLB, LLM, FTIA**

Senator Hill was born in 1946 in Adelaide. He is married with four children. He was educated at Scotch College, Mitcham, South Australia. In 1968 he obtained his law degree at the University of Adelaide (St Mark's College) and in 1970 his Masters of Law at the University of London (University College and the London School of

Economics & Political Science). He then completed a Bachelor of Arts Degree in Asian History & International Politics in 1982 at the University of Adelaide.

Senator Hill's interests include law reform (particularly taxation reform) and industrial relations, Australian and Asian history, legal and environmental education, environmental industry and small business.

Prior to his entry into politics, Senator Hill practised in both government service and in private practice, having been admitted to practise as a Barrister and Solicitor in South Australia, and admitted as a Legal Practitioner in the Northern Territory in 1970.

Senator Hill has been involved with the Liberal Party of Australia for more than 25 years and has held many positions within the party, including State President (South Australia Division) (1985–1987). He has been a member of the Federal Executive of the Liberal Party of Australia between 1985 and 1987, and since April 1990.

Elected as a Liberal Senator for South Australia in October 1980 (his term commencing on 1 July 1981), Senator Hill has been continuously re-elected in March 1983, July 1987, March 1990 and March 1996. He was elected Leader of the Opposition in the Senate on 11 April 1990.

Senator Hill held a number of shadow portfolios while in Opposition, namely:

- Shadow Minister for Justice, the ACT and the Status of Women (16 September 1988 – 12 May 1989).
- Shadow Minister for Foreign Affairs (12 May 1989 – 7 April 1993).
- Shadow Minister for Defence and Public Administration (8 April 1993 – 17 January 1994).
- Shadow Minister for Public Administration (17 January 1994 – 26 May 1994).
- Shadow Minister for Education, Science and Technology (26 May 1994 – 7 March 1996).

When John Howard and the Coalition of the Liberal Party of Australia and the National Party of Australia won Government on 3 March 1996, Senator Hill was appointed Leader of the Government in the Senate. He was also appointed Minister for the Environment and, after the 1998 election, he was given responsibility for the portfolio of Heritage. Senator Hill has been the longest-serving Environment Minister. After the Coalition was returned to Government on 10 November 2001, Senator Hill was appointed as the Minister for Defence. He has retained his office as Leader of the Government in the Senate.

## **LIEUTENANT GENERAL JOSEPH E. HURD (USAF, RETIRED)**

Lieutenant General (R) Joseph E. Hurd is currently serving as a Senior Mentor in the Chief of Staff Air Force Operational Command Training Program at Hurlburt Air Force Base, Florida.

Lieutenant General Hurd entered the United States Air Force (USAF) in 1965 through the Reserve Officer Training Corps program and completed pilot training at Webb Air Force Base, Texas, in 1966. Following F-4 training and a tour at Eglin Air Force Base, Florida, he flew 169 combat missions in South Vietnam. A command pilot with more than 3700 hours in F-4, F-15 and F-16 aircraft, he has served as a fighter weapons school instructor, operations officer, squadron commander, deputy commander for operations and wing commander.

Previous staff assignments include three tours at Headquarters United States Air Force, Washington DC; a tour at Headquarters Tactical Air Command, Langley Air Force Base, Virginia; a tour at Headquarters US Central Command, MacDill Air Force Base, Florida; and his last assignment was Deputy Commander in Chief, United Nations Command Korea; Deputy Commander, US Forces Korea; Commander, Air Component Command, Republic of Korea and US Combined Forces Command; and Commander, 7th Air Force, Pacific Air Forces, Osan Air Base, South Korea.

## **AIR VICE-MARSHAL IAIN MCNICOLL, CBE, BSC, FRAES, RAF**

Air Vice-Marshal McNicoll was appointed Director General Joint Doctrine and Concepts in June 2002. The Joint Doctrine and Concepts Centre (JDCC) at Shrivenham is part of the Ministry of Defence central policy staff; its role is to provide long-term conceptual underpinning for defence planning and develop joint doctrine. JDCC is also responsible for developing and promoting the military contribution to the UK and multinational comprehensive response to prevent or resolve conflict in international crises.

Air Vice-Marshal McNicoll joined the Royal Air Force (RAF) in 1975 and has flown over 4000 hours. His squadron and station command appointments were of No 17 (Fighter) Squadron and RAF Brüggen in Germany. His staff appointments have included being a personal staff officer to the Chief of the Defence Staff and, prior to taking up his current post, Director of Force Development. His next appointment is Air Officer Commanding No 2 Group.

## **AIR MARSHAL SUBHASH BHOJWANI**

Air Marshal Subhash Bhojwani Air is the Air Officer Commanding-in-Chief Training Command, Indian Air Force. An alumnus of the National Defence Academy, he was commissioned as a fighter pilot in the Indian Air Force in 1965. He has flown approximately 4500 hours on various fighter aircraft, including the Hunter, MiG-21, Jaguar and Mirage 2000, and a host of training aircraft. He saw action during the Indo-Pakistan war of 1971, during which he flew 31 operational missions and earned

a Mention in Dispatches. He is a fighter combat leader and a Category A1 qualified flying instructor.

Air Marshal Bhojwani graduated from the RAF Staff College in December 1980 and the Australian College of Defence and Strategic Studies in 1997. His most important appointments include command of two front-line fighter squadrons, Chief Operational Officer at the Indian Air Force Station at Ambawa, Air Officer Commanding an Air Force station equipped with Mirage 2000 and Commandant of the Air Force Academy. He has held staff appointments at Air Headquarters in the Directorates of Operations, Personnel and Air Staff Inspections, and he has discharged instructional assignments at the Air Force Academy, Fighter Training Wing, Flying Instructor School, Defence Services Staff College and College of Air Warfare. The Air Marshal held the appointment of Senior Air Staff Officer Western Air Command prior to assuming his current appointment of Air Officer Commanding-in-Chief Training Command.

### **LIEUTENANT GENERAL DATO' AZIZAN BIN ARIFFIN**

Born in Yan, Kedah Darul Aman in 1952, Lieutenant General Dato' Azizan completed his Officer Cadet training at the Royal Military College and was commissioned on 16 April 1971 in the Air Traffic Control Branch of the Royal Malaysian Air Force (RMAF). He completed his basic and advanced Air Traffic Control courses in Austria in 1971 and 1973 respectively. He has held various appointments as an air traffic controller in units such as the Joint Air Traffic Control Centre Paya Lebar in Singapore and RMAF Base Kuantan.

Lieutenant General Dato' Azizan completed his basic and advanced flying training in Australia and graduated on 7 July 1977. Since then he has flown CT4, Bulldog B 100, Aermacchi MB 326H, Cessna 402B, Pilatus PC-7, BAe 125, Fokker 28, Falcon 900 and C-130 aircraft. He was Squadron Commander of the VIP Squadron and examiner, flying instructor and Standard Officer at the RMAF Flying Training School. He was also a member of the National Aerobatic Team 'Taming Sari'. Lieutenant General Dato' Azizan has held a number of important staff, command and tri-Service appointments. He was assigned to Pakistan as Defence Adviser, and has held the appointments of Director of Training RMAF Headquarters and Chief of Staff No 2 Air Division. He then commanded No 2 Air Division and was later appointed as Commandant of the Air Force College and Commandant of the Malaysian Armed Forces Academy. He has attended numerous overseas specialist courses, local career courses and is a graduate of Air Command and Staff College (USA) and National Defence College (India).

Lieutenant General Dato' Azizan bin Ariffin assumed the appointment of Deputy Chief of Air Force on 5 April 2004.

In recognition of his service and contribution towards national security, Lieutenant General Dato' Azizan was conferred with a number of Federal, State and Armed Forces awards. Among these are the Darjah Kebesaran Sri Indera Mahkota Pahang (SIMP) and Darjah Kebesaran Sultan Ahmad Shah Pahang (DSAP), which carries the title Dato' from His Royal Highness the Sultan of Pahang; Darjah Setia DiRaja Kedah

(DSDK), which carries the title Dato' from His Royal Highness the Sultan of Kedah; Panglima Setia Angkatan Tentera (PSAT); Johan Setia DiRaja (JSD); Darjah Pahlawan Angkatan Tentera (PAT); Johan Mangku Negara (JMN) and Kesatria Angkatan Tentera (KAT) from His Majesty DYMM Seri Paduka Baginda Yang di-Pertuan Agong.

Lieutenant General Dato' Azizan is married to Datin Noorainee Abd Rahim and the couple is blessed with two daughters and three sons. He is active in sports and has a passion for golf.

## **PROFESSOR ROSS BABBAGE**

Professor Ross Babbage is Managing Director of Strategy International (ACT) Pty Ltd, a defence consulting and education service delivery organisation. Professor Babbage is also Chairman of The Kokoda Foundation, a not-for-profit organisation committed to researching Australia's most difficult future security challenges. In addition, Professor Babbage is a Council Member of the International Institute for Strategic Studies in London and an Adjunct Professor in strategic and defence studies at the Australian National University.

Professor Babbage has wide-ranging expertise in international security affairs. He has held several senior positions in the Australian Public Service, including Head of Strategic Analysis in the Office of National Assessments, and he led the branch in the Department of Defence responsible for ANZUS policy. Professor Babbage was Assistant Secretary, Force Development in the late 1980s, carrying responsibility for the analysis of all major Defence capability proposals and the preparation of recommendations for the senior Defence committees and for Cabinet. From 1986 to 1990 he was Deputy Head of the Strategic and Defence Studies Centre at the Australian National University. Through the 1990s, Professor Babbage worked with ADI Limited,<sup>1</sup> Australia's largest defence company. In the late 1990s he served as Corporate Executive Strategic Analysis, carrying primary responsibility for the company's longer term thinking and planning. In 2000 he was appointed the inaugural Director of the Centre for International Strategic Analysis in Perth. In 2003 and 2004 he served as Head of the Strategic and Defence Studies Centre at the Australian National University.

Professor Babbage has Bachelor and Masters Degrees in Economics from the University of Sydney and a PhD in International Relations from the Australian National University. He is author of *A Coast Too Long: Defending Australia Beyond the 1990s* (Allen & Unwin, Sydney, 1990), *Rethinking Australia's Defence* (University of Queensland Press, St Lucia, 1980) and *Getting Real – Reviewing Australia's Defence Capabilities* (Australian Strategic Policy Institute, Canberra, forthcoming). Professor Babbage has also written extensively on Asia-Pacific affairs focusing, in particular, on medium- and long-term regional trends.

---

<sup>1</sup> *Editor's Note:* Formerly known as Australian Defence Industries. The 'Australian Defence Industries' name was changed in January 1996 to become, simply, ADI.

## **DOCTOR ALAN VICK**

Dr Alan Vick is a senior political scientist at RAND. He has been on the RAND research staff since 1983 and has led studies for the USAF, US Army and US Defense Department on subjects ranging from military strategy to crisis management. For the USAF, he has investigated ground threats to air bases, ways to enhance aerospace operations in urban settings, against light infantry opponents, in operations other than war and against elusive ground targets. Recently, he led a study on enhancing the integration of air and ground operations. He is currently leading a study of the role of air power in counterinsurgency operations. His report on the history of ground threats to Air Force bases, *Snakes in the Eagle's Nest*, is used by the USAF as a textbook in training security forces.

Dr Vick served as Associate Director of Project AIR FORCE (2002–2004), Acting Director of the Strategy and Doctrine Program in Project AIR FORCE (2003–2004), Associate Director of the Strategy and Doctrine Program (1998–2001), Project AIR FORCE liaison to the Air Staff (1989–1994) and Assistant to the Vice President of the Arroyo Center, RAND's Army research division (1985–1986). He was an infantryman in the 82nd Airborne Division from 1973 to 1976. Alan holds a PhD (1983) in Political Science from the University of California, Irvine.

## **DOCTOR ALAN STEPHENS**

Dr Alan Stephens is a visiting fellow at both the Strategic and Defence Studies Centre, Australian National University, and the School of Humanities and Social Sciences, University of New South Wales. Previously he has been a senior lecturer at University College, Australian Defence Force Academy, where he taught courses in aerospace power history and strategy; the official Royal Australian Air Force historian; a principal research officer in the Australian Federal Parliament, specialising in foreign affairs and defence; and a pilot in the RAAF, where his service included a tour in Vietnam and an appointment as Commanding Officer of No 2 Squadron.

Dr Stephens has published widely on defence and security issues, and on air power history and strategy. He also has lectured extensively throughout Australia, Europe, the United States and South-East Asia. Dr Stephens was one of the principal authors of the third edition of the RAAF *Air Power Manual* (1998). His published works include *Going Solo: The Royal Australian Air Force 1946–1971*, an official history of the RAAF from the end of World War II to the Service's Golden Anniversary in 1971; and *The Australian Centenary History of Defence, Volume II, The Royal Australian Air Force*, published as part of the Oxford Centenary of Australian Defence series.

## **MR SANU KAINIKARA**

Mr Sanu Kainikara is a former fighter pilot of the Indian Air Force with 21 years of commissioned service and vast operational flying experience in a number of modern fighter aircraft. He is a Qualified Flying Instructor and a graduate of the Fighter

Weapons School. Currently he is the Acting Director of the RAAF Air Power Development Centre.

Prior to this appointment, Mr Kainikara taught Aerospace Engineering at the Royal Melbourne Institute of Technology University and was a consultant to the Air Operations Division of DSTO, Melbourne. He is a regular contributor to defence related magazines and has published prolifically on air power and defence issues in the *Asia-Pacific Defence Reporter*, *Fighter Tactics*, *Australian Defence Force Journal* and *The Leading Edge*. He is also a contributing editor to the *Asia-Pacific Defence Reporter*.

Mr Kainikara is a graduate of the Indian National Defence Academy, Defence Services Staff College and the College of Air Warfare. He holds two Bachelors Degrees and also a Master of Science in Defence and Strategic Studies from the University of Madras. His doctoral thesis in International Politics with the University of Adelaide is currently being evaluated.

### **LIEUTENANT GENERAL CARL O'BERRY (USAF, RETIRED)**

Lieutenant General Carl O'Berry is Vice President of the Boeing Strategic Architecture organisation in Anaheim, California, reporting to Jim Albaugh, President and Chief Executive Officer of Boeing Integrated Defense Systems. He is responsible for directing the development and application of a Boeing-wide strategic communication and information architecture that will ensure and certify interoperability of all programs for IDS and The Boeing Company.

Under Lieutenant General O'Berry's leadership, the Strategic Architecture (SA) organisation concentrates on architecture development, demonstration, modelling, simulation and distribution aimed at improving customers' mission effectiveness—both internal to Boeing and in other government, industry and civil venues. SA is also responsible for demonstrating the principles and practice of Net-Centric and Effects-Based Operations and educating Boeing leadership, engineers, program management and design teams, as well as IDS customers, on the value of Net-Centric and network enabled operations.

Previously, Lieutenant General O'Berry served as vice president and general manager of the Government Information & Communications Systems (GI&CS) business segment. In that capacity, he was responsible for leveraging systems-of-systems technologies into numerous market areas, such as global positioning/navigation systems, airborne early warning and control systems, integrated battle management systems and information operations.

Lieutenant General O'Berry joined Boeing after three years with the Motorola Space and Systems Technology Group, where he was vice president and director of planning and information technology. Before accepting the position at Motorola, he managed several large-scale Department of Defense command, control and communication and R&D programs and commanded several US Air Force organisations, including the Rome Air Development Center. He retired in the grade of Lieutenant General in 1995 after more than 38 years of service in the US Air Force.

In his last Air Force assignment, Lieutenant General O'Berry served as deputy chief of staff, Command, Control, Communications and Computers (C4), at US Air Force Headquarters in Washington DC, where he was responsible for operational policy affecting more than 55,000 US Air Force C4 personnel, and C4 systems valued at approximately US\$16 billion.

Lieutenant General O'Berry holds a Bachelor of Science Degree in Electrical Engineering from New Mexico State University and a Master of Science Degree in Systems Management from the Air Force Institute of Technology.

Lieutenant General O'Berry and his wife, Charlene, both natives of Lansing, Michigan, have two daughters and three sons.

### **GROUP CAPTAIN CHRIS FINN, RAF**

Group Captain Christopher Finn joined the RAF, from Grammar School, in 1972. After Navigator training and conversion to the Buccaneer he served, between July 1975 and November 1983, on 809 Naval Air Squadron (HMS *Ark Royal*), XV Squadron (RAF Laarbruch) and 237 Operational Conversion Unit (RAF Honington). A specialist in electronic warfare, weaponry and tactics Finn was awarded a Queen's Commendation for Valuable Service in the Air (QCSA) for his instructional duties on 237 Operational Conversion Unit.

After a short period at Headquarters 18 Group Northwood, he was promoted to Squadron Leader and posted to 208 Squadron, at RAF Lossiemouth, as Weapons Leader in July 1984. He was awarded a second QCSA for his work in introducing the Sea Eagle missile into front-line service during this tour. In January 1988 Finn moved to the Central Tactics and Trials Organisation as the Buccaneer role officer.

In 1989/90 he attended Joint Service Defence College Course 10, after which he was posted to the Headquarters Strike Command Plans Branch. In December 1990 he was promoted to Wing Commander and posted to Headquarters 18 Group, during which he served in Air Headquarters Riyadh as SO1 Bucc/UK LGB specialist for Operation *Granby*. From April to September 1992 he worked on the Air Warfare Centre (AWC) Study Team. He then spent two and a half years as Chief of Operational Studies in the AWC at RAF College Cranwell. Wing Commander Finn took command of the Air Navigation School, at RAF Finningley, in August 1995. This became the Navigator & Airman Aircrew School, at RAF College Cranwell, in January 1996. At the end of this tour he had amassed over 3200 flying hours, 2240 of those hours on the Buccaneer.

Between April 1998 and September 1999 he was the RAF member of the Joint Doctrine and Concepts Centre study, and later implementation, teams. Between October 1999 and July 2000 he undertook the Master of Philosophy in International Relations course at Cambridge University. He then spent 20 months as an air power specialist on the Directing Staff of the Joint Services' Command and Staff College. He became Director Defence Studies (RAF) on promotion to Group Captain in June 2002. Since January 2005 he has been serving in the Ministry of Defence.

Group Captain Finn and his wife Caroline live in their own home near Grantham. Their elder son is 21 and their younger son, aged 19, is at a residential school for children with severe speech handicaps, in Burton upon Trent.

Group Captain Finn's hobbies are narrowboating, cooking, swimming and bridge.

## **AIR VICE-MARSHAL JULIE HAMMER, AM, CSC**

Air Vice-Marshal Julie Hammer, an electronics engineer, is the most senior woman in the Australian Defence Force. She was the first serving woman to achieve One Star rank, on promotion to Air Commodore in 1999, and subsequently the first woman to achieve Two Star rank, on promotion to Air Vice-Marshal in 2003. She is the only woman in the history of the Australian Defence Force to have achieved 'starred' rank. She completed her schooling in Brisbane and in 1971 was placed 8th in the Queensland Senior Public (Matriculation) Examination.

She joined the Royal Australian Air Force in 1977 after completing a Bachelor of Science (Honours) in Physics at the University of Queensland. She also holds a Masters Degree in Aerosystems Engineering and a Graduate Diploma in Strategic Studies. Currently the Acting Chief Information Officer for Defence, she has served in the fields of aircraft maintenance, technical intelligence, electronic warfare, and command, control, communications and intelligence (C3I) systems acquisition and support. She was the Commandant of the Australian Defence Force Academy during 2002 and 2003.

Air Vice-Marshal Hammer was the first woman to command an operational unit in the RAAF, the Electronic Warfare Squadron, and was awarded a Conspicuous Service Cross for that command. She was the recipient of the 1996 Association of Old Crows (Australian Chapter) Award for Distinguished Service to Electronic Warfare. She was awarded the 2001 Sir Charles Kingsford Smith Memorial Medal by the Royal Aeronautical Society to recognise her contribution to Australian aerospace and delivered the 2001 Kingsford Smith Memorial Lecture. Air Vice-Marshal Hammer is a Fellow of the Institution of Engineers Australia, a Fellow of the Royal Aeronautical Society and a Graduate of the Australian Institute of Company Directors. She is one of the inaugural Board Members of the Centre for Engineering Leadership and Management within the Institution of Engineers Australia. She served for three years from 1996 to 1998 as one of the Prime Minister's representatives on the Governor General's Australian Bravery Awards Council. In 2002, she was appointed by the Minister Assisting the Prime Minister for the Status of Women to be one of Australia's Honouring Women Ambassadors. She was awarded the 2003 Alumnus of the Year of the University of Queensland to recognise her contribution to her profession and was appointed as a Member in the Military Division of the Order of Australia (AM) in the 2004 Australia Day Honours List.

Air Vice-Marshal Hammer is married to Air Vice-Marshal David Dunlop, CSC, who serves as Director General Cadets.

## **VICE ADMIRAL CHRIS RITCHIE, AO, RAN**

Vice Admiral Chris Ritchie graduated from the RAN College in 1968 and received further training at sea and in the United Kingdom before undertaking a succession of seagoing appointments and a staff appointment at the NATO School of Maritime Operations at HMS *Dryad*.

His commands have included HMAS *Tarakan*, HMAS *Torrens*, and HMAS *Brisbane*. During his period in command of HMAS *Brisbane*, the ship deployed to the Arabian Gulf, where he participated for the duration of the Gulf War. In 1991, as a result of this service, he was appointed a Member in the Military Division of the Order of Australia (AM).

In 1992, Vice Admiral Ritchie attended the Royal College of Defence Studies in the United Kingdom. On completion he was promoted to Commodore and had appointments in Naval Policy and Warfare, and Military Strategy and Concepts. In 1997 he was promoted and appointed as Maritime Commander Australia, returning to Canberra in May 1999 to serve briefly as Deputy Chief of Navy before taking up the appointment of Head of Capability Systems. As a consequence of his service in these appointments, he was promoted to Officer in the Military Division of the Order of Australia (AO) in January 2001.

Vice Admiral Ritchie was appointed as Commander Australian Theatre on 3 August 2001. He was the first Commander to have previously served as a Component Commander to the Headquarters. On 3 July 2002, he was appointed as Chief of Navy and promoted to Vice Admiral.

Vice Admiral Ritchie is married to Julia and has two adult sons.

## **LIEUTENANT GENERAL PETER LEAHY, AO**

Lieutenant General Leahy was born on 30 October 1952 in Melbourne. After completing his secondary education at Aquinas College in Melbourne, he entered the Royal Military College in 1971, graduating in 1974 into the Royal Australian Infantry Corps. His initial appointment was as a Platoon Commander in 8/9 Battalion of the Royal Australian Regiment (8/9 RAR). He further served with the Regiment as Second-in-Command of 5/7 RAR (Mechanised), and Commanding Officer of 8/9 RAR. From 1997 to 1999 he commanded the 3rd Brigade, the Rapid Deployment Force in Townsville.

From 1981 until 1982 Lieutenant General Leahy served on exchange with the British Army in Hong Kong as Operations Officer and as a Company Commander in the 10th Princess Mary's Own Gurkha Rifles.

His training appointments have included postings as Instructor Infantry at the Officer Cadet School, Portsea, and Instructor Tactics at the Infantry Centre, Singleton. From 1987 to 1990 he was posted as the Australian Exchange Officer at the United States Army Command and General Staff College, Fort Leavenworth, where he instructed in Joint and Combined Operations and Counter Revolutionary Warfare.

Lieutenant General Leahy has previously served in Army Headquarters as the Military Assistant to the Chief of the General Staff in 1993, following which he was the Director of Army Research and Analysis in 1994 and 1995. Prior to his appointment as Deputy Chief of Army in May 2000, he was Chief of Staff at Headquarters Australian Theatre in Sydney.

Lieutenant General Leahy is a graduate of the Australian Army Command and Staff College, the United States Army Command and General Staff College, the British Higher Command and Staff Course, and is a Fellow of the Australian College of Defence and Strategic Studies. As a graduate of the University of New South Wales he was awarded a Bachelor of Arts Degree in Military Studies in 1974, and he completed a Master of Military Arts and Science Degree while at the United States Army Command and General Staff College.

Lieutenant General Leahy was advanced as an Officer in the Military Division of the Order of Australia (AO) in the Queen's Birthday Honours List in 2002, having previously been appointed a Member in 1995 for his service as the Director of Army Research and Analysis. For his service at Fort Leavenworth, he was awarded the United States Army Meritorious Service Medal.

Lieutenant General Leahy assumed his current appointment as Chief of Army on 28 June 2002.

Lieutenant General Leahy and his wife, Lee, have three sons. His leisure interests include running, military history and following almost all sports.

## **SQUADRON LEADER TIM ANDERSON**

Squadron Leader Tim Anderson was born in South Africa in 1973, and immigrated to Australia in 1981. He attended school in Adelaide, South Australia, and gained a Bachelor of Arts Degree, followed by First Class Honours in Classical Military Historiography, from the University of Adelaide.

Squadron Leader Anderson joined the Royal Australian Air Force in 1995 as a Ground Defence Officer. He attended the Royal Military College of Australia (Duntroon), graduating as a Flying Officer. He completed the Australian Army Infantry Regimental Officer Basic Course at Singleton NSW, prior to his first posting as No 1 Rifle Flight Commander at No 2 Airfield Defence Squadron.

In 1996, he was posted as a Rifle Flight Commander at the newly formed No 3 Airfield Defence Squadron at RAAF Base Amberley, and in 1997 he became the Executive Officer of that unit. In 1998 Squadron Leader Anderson was posted as the Ground Defence and Specialist Training Officer at No 1 Recruit Training Unit at RAAF Base Edinburgh in South Australia. During this time he was awarded a Commendation from Commander Training – Air Force for his work in redesigning the recruit training syllabus.

In 2000, he was posted as the Executive Officer of No 1 Airfield Defence Squadron, also at RAAF Base Edinburgh. In January 2002, Squadron Leader Anderson was

posted as Aide-de-Camp to Chief of Air Force, Air Marshal Angus Houston. Squadron Leader Anderson took up his current position in International Engagements in Air Force Headquarters in January 2003.

He is married to Bianca, and has a three-year-old daughter, Sophie. He has a passion for Rugby Union and enjoys sailing and reading classical literature in his spare time.

## **SQUADRON LEADER CHERYL NEAL**

Squadron Leader Cheryl Neal was born in Nowra, NSW. She enlisted in the Royal Australian Air Force in 1987 as a Medical Assistant, and has enjoyed postings to No 3 Hospital and to Base Squadron Tindal.

She was commissioned in 1992 and completed No 113 Basic Air Traffic Control Course. She was posted to RAAF Base Richmond as a Tower Controller, and then in 1994 to RAAF Base Pearce.

In 1999 Squadron Leader Neal was posted to Directorate of Reserves – Air Force in the Cadet Personnel Management position. During this time Squadron Leader Neal completed a Masters of Business & Technology qualification, and transferred to the Administration Officer category.

On completion of her posting to the Directorate of Reserves – Air Force, Squadron Leader Neal took up a position in the Air Operations section within the Directorate of Personnel Officers – Air Force, where she was employed to facilitate the postings of junior pilots.

In December 2002, Squadron Leader Neal commenced a posting as the Administration Officer of No 34 Squadron, and during this time participated in a deployment to the Middle East.

Squadron Leader Neal took up her current position as Staff Officer to the Director General Strategy & Planning – Air Force and Director General Capability Management – Air Force in Air Force Headquarters in November 2003.

She and her partner, Dale, have seven-year-old twin daughters, Kate and Sarah. In her spare time Squadron Leader Neal enjoys horse riding and writing both short stories and novels.

## **SQUADRON LEADER DOMINIC SIMS**

Squadron Leader Sims graduated from the Australian Defence Force Academy (ADFA) in 1989. He completed an Aeronautical Engineering Degree at the Royal Melbourne Institute of Technology in 1990. He spent 1991 completing specialist Air Force engineering and armament courses, and was posted to the Aircraft Research and Development Unit (ARDU) in January 1992 as an armament test engineer.

During this period he gained test and evaluation experience on a number of weapons test programs for F/A-18, F-111 and P-3 aircraft. In 1994, he was posted to Aircraft Stores Compatibility Engineering duties with ARDU. During this period he was responsible for stores certification activity on F/A-18 aircraft.

In late 1996, he was posted to the USAFEX1 exchange position in the United States Air Force SEEK EAGLE Office at Eglin Air Force Base in Florida. During the period December 1996 through December 1999, he managed A-10 and F-15E stores certification activities within the SEEK EAGLE Office.

Upon return to Australia in July 2000, he was promoted to Squadron Leader and posted to the AGM-142E acquisition project as the project engineering manager.

Squadron Leader Sims was posted to the Australian Command and Staff College in January 2002. Upon completion of staff course, he was posted to his current position of Staff Officer – Space Future Concepts in the Air Power Development Centre.

Squadron Leader Sims' hobbies include mountain biking, skiing and sea kayaking.

## **AIR VICE-MARSHAL ROXLEY MCLENNAN, AM**

Air Vice-Marshal McLennan was born in Hobart, Tasmania on 4 August 1950 and graduated from the RAAF Academy, RAAF Point Cook, Victoria, in December 1971. He holds the degrees of Bachelor of Science (Physics) from Melbourne University (1971) and Master of Science (Logistics Management) from the United States Air Force Institute of Technology (Class of '84). He graduated from the Australian Joint Services Staff College in 1991, is a Fellow of the Australian College of Defence and Strategic Studies (1997) and a Fellow of the Royal Aeronautical Society. In 2002 he completed the Advanced Management Program at the Harvard Business School and is a Member of the Australian Institute of Company Directors.

On completion of pilot training in April 1973, Air Vice-Marshal McLennan flew the C-130A Hercules with No 36 Squadron. In April 1977 he graduated from the RAAF Central Flying School as a qualified flying instructor and flew the CT4A Airtrainer at No 1 Flying Training School, the Scottish Aviation Bulldog at RMAF Base Alor Setar while on loan to the Royal Malaysian Air Force, and subsequently returned to Australia to instruct on the Hercules C-130E of No 37 Squadron.

Air Vice-Marshal McLennan's leadership appointments include Training Flight Commander and Commanding Officer No 37 Squadron, Commander Operational Support Group, Commander Air Lift Group and Commander Integrated Area Defence System in Butterworth, Malaysia. During his tenure as Commander Air Lift Group he also served in Dili, East Timor as the Combined Air Component Commander for the International Force East Timor (INTERFET) and the Commander of the Australian Forces in East Timor (COMASC). He was appointed a Member in the Military Division of the Order of Australia (AM) for exceptional service in East Timor.

Air Vice-Marshal McLennan has also served in staff appointments in the Materiel and Personnel Divisions of the Department of Defence (Air Force Office), as the

Australian Air Adviser in London, as Director Strategic Policy and Planning – Air Force, as the Director-General Career Management Policy within the Defence Personnel Executive and briefly as Head Defence Personnel Executive. On 1 March 2004, Air Vice-Marshal McLennan was appointed to his present position of Deputy Chief of Air Force.

Air Vice-Marshal McLennan is married to Loretta and they have four children, Cameron, Andrea, Michelle and Philip. He enjoys flying, golf and live theatre.

## ABBREVIATIONS

AAA	Anti-Aircraft Artillery
AAR	Air-to-Air Refuelling
AC2ISR	Aerospace Command, Control, Intelligence, Surveillance and Reconnaissance [Center] [US]
ACO	Airspace Control Order
ACT	Australian Capital Territory
ACTD	Advanced Control Technology Demonstration
ADDP	Australian Defence Doctrine Publication
ADF	Australian Defence Force
AEW&C	Airborne Early Warning and Control
AFC	Air Force Cross
AFV	Armoured Fighting Vehicle
AIRCENT	Allied Air Forces Central Europe
AM	Member of the Order of Australia
AMRAAM	Advanced Medium-Range Air-to-Air Missile
ANZUS	Australia, New Zealand and United States
AO	Area of Operations
AO	Officer of the Order of Australia
AOC	Air Operations Centre
AOD	Air Operations Directive
ARDU	Aircraft Research and Development Unit
AS	Australia
ASRAAM	Advanced Short-Range Air-to-Air Missile
AT3	Advanced Tactical Targeting Technology
ATAF	Allied Tactical Air Force
ATM	Air Task Message
ATO	Air Tasking Order
ATOC	Allied Tactical Operations Centre
AUSCANNZUKUS	Australia, Canada, New Zealand, United Kingdom and United States
AWACS	Airborne Warning and Control System
AWD	Air Warfare Destroyer
BDA	Battle Damage Assessment
BOS	Battlespace Operating System
BSc	Bachelor of Science
C2	Command and Control
C3	Command, Control and Communications
C3I	Command, Control, Communications and Intelligence
C4	Command, Control, Communications and Computers
C4I	Command, Control, Communications, Computers and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance

CA	Chief of Army
CAF	Chief of Air Force
CAOC	Combined Air Operations Centre
CAS	Close Air Support
CBE	Commander of the Order of the British Empire
CBM	Command and Battlespace Management
CBRN	Chemical, Biological, Radiological and Nuclear
CCDG	Chief Capability Development Group
CCNW	Counter-Counter Network Warfare
CCT	Combat Controller
CDS	Chief Defence Scientist
CEC	Cooperative Engagement Capability
CENTCOM	Central Command [US]
CEO DMO	Chief Executive Officer Defence Materiel Organisation [AS]
CEP	Circular Error Probable
CFO	Chief Finance Officer [AS]
CINC	Commander-in-Chief
CIO	Chief Information Officer [AS]
CIS	Communication and Information Systems
CJOPS	Chief of Joint Operations [AS]
CN	Chief of Navy
CNW	Counter Network Warfare
COMAIRSOUTH	Commander Allied Air Forces Southern Europe
COMAO	Composite Air Operation
CONOPS	Concept of Operations
COP	Common Operational [or Operating] Picture
CP	Command Post
DCGS	Distributed Common Ground System
DCP	Defence Capability Plan [AS]
DCTS	Defense Collaboration Tool Suite [US]
DEAD	Destruction of Enemy Air Defences
DEPSEC CS	Deputy Secretary Corporate Services [AS]
DEPSEC I&S	Deputy Secretary Intelligence and Security [AS]
DEPSEC S	Deputy Secretary Strategy [AS]
DIE	Defence Information Environment [AS]
DIEC	Defence Information Environment Committee [AS]
DJC2	Deployable Joint Command and Control
DMFP	Defence Management Financial Plan [AS]
DMO	Defence Materiel Organisation [AS]
DoDAF	Department of Defense Architecture Framework [US]
DSTO	Defence Science and Technology Organisation [AS]
EBO	Effects-Based Operations
EBS	Effects-Based Strategy
ECCM	Electronic Counter-Countermeasures
ECM	Electronic Countermeasures
ELINT	Electronic Intelligence
ESD	Electronic Systems Division [AS]
ETAC	Enlisted Terminal Attack Controller

EW	Electronic Warfare
FAC	Forward Air Controller
FLOC	Future Land Operating Concept [AS]
FO	Forward Observer
FRAeS	Fellow Royal Aeronautical Society
FSCL	Fire Support Coordination Line
FTIA	Fellow Taxation Institute of Australia
GCCS	Global Command and Control System
GIG	Global Information Grid
GPS	Global Positioning System
HARM	High-Speed Anti-Radiation Missile
HDPE	Head Defence Personnel Executive [AS]
HF	High Frequency
HLOC	High Level Operational Concept [UK]
HMAS	Her Majesty's Australian Ship
HMS	Her Majesty's Ship
HNA	Hardening and Networking the Army [AS]
HTACC	Hardened Tactical Air Control Center [US]
IADS	Integrated Air Defence System
IAF	Indian Air Force
ICD	Information Capability Development
ID	Identification
IDM	Improved Data Modem
IFF	Identification Friend or Foe
IMINT	Imagery Intelligence
IP	Internet Protocol
IPB	Intelligence Preparation of the Battlespace/Battlefield
ISD	Information Systems Division [AS]
ISR	Intelligence, Surveillance and Reconnaissance
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
IT	Information Technology
IWS	InfoWorkSpace
JDAM	Joint Direct Attack Munition
JDCC	Joint Doctrine and Concepts Centre [UK]
JEFX	Joint Expeditionary Force Experiment [US]
JFACC	Joint Force Air Component Commander
JFC	Joint Force Commander
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JFSOCC	Joint Force Special Operations Component Commander
JOP	Joint Operational Picture
JORN	Jindalee Over-the-Horizon Radar Network
JP	Joint Project [AS]
JSF	Joint Strike Fighter

JSTARS	Joint Surveillance and Target Attack Radar System
JTFC	Joint Task Force Commander
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
JTTP	Joint Tactics, Techniques and Procedures
JWID	Joint Warrior Interoperability Demonstration
LLB	Bachelor of Laws
LLM	Master of Laws
LPA	Amphibious Transport
MANPADS	Man-Portable Air Defence System
MASINT	Measurement and Signature Intelligence
MC2A	Multi-Sensor Command and Control Aircraft
MIDS	Multifunction Information Distribution System
MIF	Maritime Interception Force
MMA	Multi-Mission Aircraft
MNTG	Multinational Naval Task Group
MOD	Ministry of Defence [UK]
MODAF	MOD Architecture Framework [UK]
MP-CDL	Multi-Platform Common Data Link
MP-RTIP	Multi-Platform Radar Technology Insertion Program
MTI	Moving Target Indicator
NATO	North Atlantic Treaty Organisation
NBC	Nuclear, Biological and Chemical
NCCT	Network Centric Collaborative Targeting
NCO	Network Centric Operations
NCOIC	Network Centric Operations Industry Consortium
NCW	Network Centric Warfare
NEC	Network Enabled Capability
NITEWorks	Network Integration Test and Experimentation Works [UK]
NTDS	Naval Tactical Data System
OODA	Observe, Orient, Decide, Act
OOTW	Operations Other Than War
PBA	Predictive Battlespace Awareness
PhD	Doctor/Doctorate of Philosophy
RAAF	Royal Australian Air Force
RAF	Royal Air Force
RAMSI	Regional Assistance Mission to Solomon Islands
RAN	Royal Australian Navy
RAPID	Rapid Prototyping Development and Evaluation Program
RAR	Royal Australian Regiment
RAWS	Radar Attack and Warning System
RDP	Radar Data Processing
REA	Rapid Environmental Assessment
RFC	Royal Flying Corps

RMAF	Royal Malaysian Air Force
RMCS	Royal Military College of Science
RN	Royal Navy
RPG	Rocket Propelled Grenade
RSAF	Republic of Singapore Air Force
SA	Situational Awareness
SADL	Situational Awareness Data Link
SAM	Surface-to-Air Missile
SAR	Search and Rescue
SAR	Synthetic Aperture Radar
SATCOM	Satellite Communications
SDR	Strategic Defence Review [UK]
SDSS	Standard Defence Supply System [AS]
SEAD	Suppression of Enemy Air Defences
SIGINT	Signals Intelligence
SINCGARS	Single Channel Ground and Airborne Radio System
SIPRNET	Secret Internet Protocol Router Network
SITREP	Situation Report
SMS	Short Message [or Messaging] Service
SOF	Special Operations Forces
TAC	Terminal Attack Controller
TBMCS	Theatre Battle Management Core System
TTNT	Tactical Targeting Network Technology
TTP	Tactics, Techniques and Procedures
UAV	Unmanned [or Uninhabited] Aerial Vehicle
UCAV	Unmanned [or Uninhabited] Combat Aerial Vehicle
UHF	Ultra High Frequency
UK	United Kingdom
UN	United Nations
US	United States
USAF	United States Air Force
USMC	United States Marine Corps
USN	United States Navy
USS	United States Ship
VCDS	Vice Chief of the Defence Staff [UK]
VMF	Variable Message Format
VTC	Video Teleconference
WG	Working Group
WMD	Weapons of Mass Destruction
W/T	Wireless Transmission
XML	Extensible Markup Language



# WELCOME ADDRESS

## AIR MARSHAL ANGUS HOUSTON, AO, AFC

Senator the Honourable Robert Hill, Minister for Defence, visiting Chiefs of Staff and senior officers, distinguished guests, ladies and gentlemen. I would like to extend a very warm welcome to all of you to the 2004 Royal Australian Air Force Air Power Conference. It is great to see so many people here and I am sure you will have a good experience over the next two days. I am delighted that so many people have come to what promises to be a thought provoking and forward thinking conference on network centric warfare and the future of air power. I look forward to the presentations and, hopefully, some lively and stimulating debate and discussion during the course of the next two days. I am particularly pleased to welcome Air Force Chiefs and their representatives from around the world. I also welcome our speakers, whose contributions and original thinking are vital to the success of this conference. Some have travelled long distances to be here and have accommodated our requirements within extremely busy schedules. I am, therefore, very grateful for their support.

*Network Centric Warfare and the Future of Air Power* is the eighth in the Royal Australian Air Force's biennial series of conferences. Since our last conference in 2002 we have seen significant changes in the international security scenario. We have seen the success of Operation *Falconer* and the gradual move forward in Iraq towards the beginning of democracy. We have also seen a marked rise in the incidence of terrorist activities, as well as its spread to hitherto peaceful areas. The recent terrorist outrages in the small town of Beslan in Russia, and in Jakarta, are the latest in a series of atrocities that have shocked the world in the last few days. It is with this backdrop that we commence our discussions in Canberra on this peaceful spring day.

In the past decade, warfighting concepts and applications have become increasingly joint. The need to have effective battlespace management, sophisticated information, surveillance and reconnaissance capabilities, and efficient command and control assets have never been more of a priority. Networking the force—the Australian Defence Force and, within it, the Air Force—therefore, takes on added importance. This conference is poised to inquire into network centric warfare within the overall strategic environment and then to focus on what the future might have in store for air power. I anticipate intellectually stimulating presentations from our distinguished speakers and, even more, a lively debate on each point that is being made, especially from the younger members of the Australian Defence Force. I commend the proceedings to you.

I should also note here that conferences of this magnitude do not happen without the active support from the private sector. I am delighted to thank our principal sponsor, Boeing; major sponsors, Rolls-Royce and Qantas; and other sponsors Defence Force Credit Union, Defence Health and ID Warehouse for their wholehearted support. To all of them, thank you for making this conference possible; I acknowledge and deeply appreciate your generosity.

Before I finish I have one final and all-important task to perform. We are privileged today to have the Minister for Defence, the Honourable Robert Hill, to open the conference by broadly outlining the ADF Roadmap for network centric warfare. I am most grateful that the Minister is available to come here this morning during an exceptionally busy time in his schedule.

Now, without further ado, we will commence the proceedings of the conference. Please sit back, relax and enjoy an intellectual feast, and insights into network centric warfare and the future of air power.

Ladies and gentlemen, please welcome the Minister for Defence to open the Royal Australian Air Force's 2004 Air Power Conference *Network Centric Warfare and the Future of Air Power*.

# **OPENING ADDRESS**

## **NETWORK CENTRIC WARFARE THE ADF ROADMAP**

**SENATOR THE HONOURABLE ROBERT HILL,  
BA, LLB, LLM, FTIA**

Air Marshal Houston, visiting Air Chiefs, distinguished guests, ladies and gentlemen, at the outset, I welcome the representatives of allied and friendly nations who have come to participate in this biennial event organised by the RAAF. Your presence here demonstrates Australia's determination to work closely with nations interested in preserving peace and international order.

This conference is an important event, not only for the RAAF but for the entire Australian Defence Force, because it aims to look at Network Centric Warfare (NCW) and the Future of Air Power, both of which are at the forefront of overall defence competence.

The global security scenario is in a state of flux and our own strategic environment is becoming more complex and uncertain.

Our military forces will have to be ready to face a wide range of contingencies at short notice. There has been ample proof of this in recent times. This will require a broad suite of capabilities that will be optimised by leveraging all possible force multipliers.

We have not, until recent years, had to play a significant role in countering terrorist threats or responding to terrorist attacks. That has now changed.

In our own region I am pleased that the Five Power Defence Arrangements have been extended to allow for a joint response to terrorist activities in South-East Asia. This is a position we promoted at the last two Ministerial meetings. It does not mean that we will necessarily be called upon to help. It does, however, mean that the defence forces, and particularly the air forces, of the five nations will jointly train for such a requirement. It means that we can also engage other states—global powers, such as the United States, and littoral states, such as Indonesia—in such exercises.

Collective action is the best way of deterring and defeating terrorism.

As a concrete and current example of this, Exercise *Bersama Lima* is presently in progress in the South China Sea. The exercise involves five countries, more than 31 ships, 60 aircraft, two submarines and over 3500 personnel. It will for the first time specifically involve maritime counter-terrorism interdiction activities.

I am also pleased that the RAAF is now able again to exercise with Indonesia in maritime surveillance. I have been pressing my Indonesian counterparts on the potential value of joint maritime surveillance. The planned exercise will be a significant step forward on that path, which would be a very positive development in both our interests.

Maritime surveillance will continue to be of critical importance. The upgrades of our AP-3C aircraft have resulted in them becoming arguably the best maritime surveillance aircraft in the world. The cooperative maritime surveillance we do in the region, such as the Operation *Gateway* patrol programs out of Butterworth in Malaysia, are a valuable asset for Australia and our regional friends, as we address common threats.

As you would also know, we have been a leader in the development of the Proliferation Security Initiative, which is designed to counter the transfer of weapons of mass destruction or their precursors. Whilst illegal transfers between states are a major worry, our ultimate concern is a transfer to a non-state player.

We hosted the first maritime interdiction exercise in the Coral Sea last year. Further exercises in East Asia and South-East Asia are now planned, and more regional states are becoming engaged. The intelligence, training and doctrine being developed under this initiative will also assist the regional states in meeting common threats. Air surveillance is a critical part of these exercises.

Our C-130 tactical transport aircraft remain a vital component in any Australian contribution to a terrorist incident in the region. And of course the response of these aircraft and crews in rescue and support after the Bali attacks was really magnificent.

The engagement of our Special Forces in regional counter-terrorism continues to grow. The recent regional counter-terrorism conference we hosted was a great success. The presence of Indonesian forces was another step in the right direction.

The emphasis of the meeting was on cooperation and mutual support. We conduct exercises with Singapore, Thailand, Malaysia and the Philippines. Again, our C-130s are the preferred transport, and with night vision capabilities and protection against shoulder-fired weapons their capability continues to grow.

Returning to the subject of multipliers. The explosion in the availability and exploitation of information technology over the past two decades has significantly altered the way military forces are employed. The ADF is no exception. NCW permits the ADF to adapt fully to the needs of information age warfare. It provides a huge advantage in the availability of timely, relevant and protected information. It significantly improves the likelihood of operational success.

The ADF has developed a roadmap to achieve a networked force. The roadmap is a dynamic document, which will be tailored to incorporate the lessons of real world experience. It also has the built-in capability to exploit the opportunities presented by the introduction of new technologies. The emphasis of the roadmap is on optimising the way in which people, systems and platforms link with each other and contribute to achieving the desired effect. While it focuses on the immediate future in terms of

capability development and delivery, there is also a broad vision of the longer-term future embedded within the roadmap.

The ADF has already made significant strides in harnessing the power of NCW. Last month, an NCW Program Office was created within General Hurley's Capability Development Group to better integrate Defence Capability Plan projects into an NCW architecture.

I am pleased to announce today the creation of a Rapid Prototyping Development and Evaluation Program. RAPID, as it is known, will address key NCW questions challenging Defence.

Importantly, RAPID will bring together Defence and industry in an innovative and collaborative way to accelerate the insertion of NCW capabilities into the Australian Defence Force. Presently, ADI,<sup>1</sup> BAE Systems Australia, Raytheon, SAAB and Tenix have agreed to join Defence in creating this program, and I have allocated resources of more than \$10 million dollars in the first year of operation. Details of the program will be provided to the broader industry community via Defence briefings in coming weeks. Suffice to say now that this initiative has the potential to change significantly the way in which capability development is looked at within the ADF—and it will certainly bring benefits to both small and large Defence industry players.

The program will add to what is already being done. The ADF is currently in the process of either acquiring or incorporating new technologies into its existing capabilities. Surveillance, reconnaissance and electronic warfare capabilities, as well as communications and information processing, all critical elements of the network, are being upgraded. The proposed acquisitions, such as the Joint Strike Fighter, Air Warfare Destroyer and Future Land Offensive Support System, will facilitate further development of NCW.

I would like to briefly mention the Joint Strike Fighter (JSF) and why I think the capability that JSF brings is vital for Australia and our emerging NCW capability. Our recent involvement in the events in Afghanistan and Iraq have brought home the lesson that while air, ground and maritime supremacy are essential, information superiority is the most critical element to success.

The JSF incorporates true fifth-generation stealth, and sophisticated electro-optical, radar and electronic warfare systems. These will ensure its survival on the 'first day of the war' with much greater certainty than is the case with our current air defence and strike systems. The stealth design in combination with the most advanced radar technology will permit the JSF to obtain the first shot opportunity in beyond visual range combat. Its advanced sensor suite and weapon load will also make JSF the ultimate precision air-to-ground strike option for the foreseeable future. JSF will see first, shoot first and strike first—because it will be fully network enabled.

In addition, key networking capabilities in the guise of the Wedgetail AEW&C, which was test flown in Seattle earlier this year, and the new generation A330 tanker will

---

<sup>1</sup> Formerly known as Australian Defence Industries. The Australian Defence Industries name was dropped in January 1996 to become, simply, ADI.

further improve the performance envelope of the JSF. The combination of these platforms in a networked environment will provide the ADF with a formidable air power capability that will serve Australia well into this century.

The centre barrel replacement of our F/A-18s will extend their service life and the upgrade of their weapon suite with the acquisition of the AMRAAM and ASRAAM missiles will ensure a greater operational capability for the aircraft. A few weeks ago the Government took another step in acquiring long-range, stand-off missiles, to further the RAAF's strike capability. This stand-off weapon delivery capability is being given to both the AP-3C Orion and F/A-18. Combined with the operational debut of AEW&C, these enhancements will ensure that the RAAF will have unbroken capability in all spheres of its activity. There will be no 'gaps' in our air combat capability when legacy systems are retired at the end of their useful service life.

However, nothing ever stands still. Whilst I have praised the capability of the AP-3C surveillance aircraft in this address, we are already looking to its successors. The Government has recently approved technical discussions with the US on the Multi-Mission Aircraft (MMA).

It is early days, but it is already important to identify particular strengths Australia can bring to the table. Over the last couple of years, successes in the Fincastle anti-submarine warfare competition, and the first-class performance of our crews on operations have demonstrated that our maritime patrol capabilities are at the cutting edge. This operational expertise, combined with capabilities such as the leading edge work of DSTO on sensor technologies, would provide valuable contributions to the MMA project.

We are, of course, also particularly interested in industry opportunities. I think we have shown through our JSF industry support that we are committed to building a sophisticated and competitive aeronautical development and support industry in Australia, albeit within niche areas of capability.

The fact that the MMA will be built around the Boeing 737 platform—common to both our AEW&C and Special Purpose [VIP] Aircraft—should combine with our existing good relationship with Boeing, to help facilitate these opportunities.

The MMAs will be complemented by maritime surveillance UAVs, which will be another new and exciting step forward for the ADF. Some of you will recall we have done transcontinental trials of the American Global Hawk system and it shows great promise as a maritime and land surveillance platform. I am sure that these long-range surveillance UAVs will have far-reaching consequences in the way we develop air power as well as how we employ it in the future.

We have asked a lot of the RAAF in the last few years and the response has been of the highest order. Last Saturday, our C-130Hs returned to Richmond from service in the Gulf and Iraq. During their deployment, the air and ground crews of No 36 Squadron completed more than 1100 flights, carried in excess of 13 million pounds of cargo, and transported more than 15,000 people (including the Iraqi Olympic Team). As a measure of their achievement, No 36 Squadron represented

approximately two per cent of the airlift capacity, but moved somewhere between seven and eight per cent of the total cargo.

Shortly before the return of the C-130H aircraft, we had farewelled our C-130Js for their first operational deployment into Iraq—with electronic warfare enhancements having been fitted in record time.

The AP-3C Orions now conduct surveillance for troops on the ground in Iraq, as well as fulfilling their conventional maritime surveillance role. They have developed a whole new niche of capability.

Our Boeing 707 refuellers might be aged, but I personally experienced the refuelling task they undertook over Afghanistan, which was much appreciated by our Coalition allies.

The F/A-18s and crews were faultless in their contribution to the combat phase of the war in Iraq.

The Caribous played a vital role in the highly successful RAMSI mission in the Solomon Islands. And I have spoken earlier of the critical role the RAAF is playing in countering terrorism in our own region.

The RAAF has worked extraordinarily hard in recent years and made a wonderful contribution to the security of Australia and Australian interests.

As for the future, the RAAF is today poised at the beginning of an exciting new era. There are a number of new systems in the pipeline and progress to upgrade existing systems and enhance others in accordance with changing priorities. Together, they will build our capability, particularly from the network perspective.

The challenge now is for us to ensure that capabilities being brought in are utilised in a manner that gives us the maximum advantage with minimum risks. The focus has to be in identifying the critical areas and understanding the disparate systems that interact within the network that are potent and capable of timely reaction.

The success or otherwise of a network will depend on how individuals apply their skills. This in turn will drive training, education and knowledge levels to influence attitude and develop experience.

In conclusion, the RAAF today is a powerful force that, in conjunction with its sister Services, gives Australia assured protection. It is the Government's primary objective to ensure the continued operational capability of the force in a period of strategic uncertainty. A broad suite of capability will be necessary to achieve that goal. We believe that the acquisition program to which we have committed meets the requirement and complements the skills and professionalism of the men and women of the force.

I thank the Chief of Air Force, Air Marshal Houston, for the opportunity to be part of this important occasion. I commend the proceedings of the next two days to all of you and now have pleasure in formally opening the 2004 RAAF Air Power Conference.



# KEYNOTE ADDRESS

## THE FUTURE OF AIR POWER RAAF RESPONSE TO THE ADF ROADMAP

AIR MARSHAL ANGUS HOUSTON, AO, AFC

Thank you Senator Hill for your presentation.

As Senator Hill said, building a networked force provides a clear way ahead for ADF capability development. A networked force can become a source of immense power, provided that the opportunity offered can be properly harnessed. My aim in this address is to describe what Air Force is doing to make sure that the opportunity offered is properly harnessed.

Minister, Air Chiefs, delegates, ladies and gentlemen. Welcome again to this, our eighth biennial Air Power Conference, *Network Centric Warfare and the Future of Air Power*.

Many in the audience will recall the 2002 Conference, *Conflict, the State and Aerospace Power*. The intent of that conference was to explore the emerging security environment and its implications for air and space power. This year's conference, focused on Network Centric Warfare (NCW) and its relationships to air and space power, is a foil to the last. In this conference, we seek to examine ways we can respond to the demands of the security environment through the lens of NCW.

Before I turn to the direct subject of this address, that is the Australian Defence Force's NCW Roadmap and the Air Force's response to it, I will make one central observation.

I have been Chief for just over three years now and I have had the privilege of commanding the people of the Royal Australian Air Force over a most eventful period. The RAAF has undertaken operations in East Timor, Bougainville, Afghanistan, Iraq and the Solomon Islands. We have flown surveillance of our northern approaches to counter illegal immigration and illegal exploitation of our Economic Exclusion Zone. We have countered illegal fishing thousands of kilometres offshore in the Southern Ocean. We have flown first aid and relief into Baghdad, Iran, and Niue. Significantly, we also conducted emergency medical and aeromedical evacuation operations as part of Operation *Bali Assist* after the terrorist attack on 12 October 2002. We sustained the Coalition air traffic control system in Baghdad from the fall of Saddam Hussein until very recently.

Our operational tempo has been high. Through all of these deployments, our dedicated and professional combat support personnel have provided vital functionality at our forward operating bases. This has enabled our operational successes in theatres from Baghdad to Bougainville. I am very proud of my Air Force people, and indeed

the whole Australian Defence Force and its supporting infrastructure. For a small force, we have been punching above our weight.

One of the reasons the Air Force can punch above its weight is because of the quality of its people. Throughout history, Australians have consistently proven themselves people of worth in the crucible of conflict. Our Air Force predecessors from World War II, Korea, Vietnam and the Cold War set us a fine standard, which our people today continue to uphold.

Our attributes and skills are manifold, but in particular our capacity to adapt, innovate, and get along with people from other cultures has been critical to our success. That same skill set is central to success in considering a networked force, because a networked force is essentially about relationships. There are the strict systemic protocols between sensor, shooter, the command and control system, and the people that utilise them. But the key to NCW is the relationships engendered by people through the net. Simply, I think it is clear that if we want NCW to work, if we want an Australian Defence Force 'fit for purpose' to meet Australia's security needs for the 21st century, then people and their relationships will be at the centre of it. That idea has been central to sustaining the values-led Air Force we have been promoting over the last few years. In the quality of our people and our leadership system, the Air Force is already advantaged. Building from that foundation will allow us to create a networked ADF that gives the Government more options for action.

Before I move on, I want to emphasise that I see NCW as a people-centric activity. Conflict is a people-centric activity. Peace is a people-centric activity. Machines are but proxies, albeit useful, but hardly an end of themselves. The human dimension of conflict is enduring, and the part that ultimately matters. People are what matter the most to my leadership team and me.

Linking the idea of the centrality of people to effective NCW, it is important to establish early that NCW systems are primarily directed at:

- gathering and fusing data,
- shaping it to enable superior and speedy human decision-making,
- providing a mechanism to have those decisions translated into a series of linked actions to produce the desired effect on the adversary, and
- developing robust feedback mechanisms and pertinent measures of effectiveness.

A good military NCW capability can exercise this loop for holistic conflict management, and can do it in parallel with other national actions. It is all part of the national effects-based approach we have developed in our current doctrine.

However, the second point listed, enabling superior human decision-making, is central to successful conflict management and one of the key attributes of an effectively networked force. Superior decision-making is directed at getting inside the

adversary's decision cycle so that we can control, or at least influence, the shape and tempo of operations to our ends.

But to make superior decisions, you need a well-trained and educated workforce. If they are effectively networked for peace, war or anything in between, so much the better. So, returning to my focus on people and relationships as the key to effective networking, I would like to introduce Air Force's *Learning 2020* Project.

Air Force's *Learning 2020* Project is an initiative of Training Command. The intent is to support Air Force capability by exploiting learning technologies and strategies compatible with the future needs of our workforce. The outcomes of the Air Force *Learning 2020* Project have been designed to have a direct bearing on the ADF's people capability.

We intend that education and training will be transformed to embrace leading edge practices and systems. We envisage a learning system making greater use of e-learning, embedded training in workplace equipment and infrastructure, and joint learning ventures. Ultimately, we may have in place a 'virtual campus', where learning could take place anywhere, at any time, providing a flexible capacity to quickly up-skill our people as needed. Again, the focus is on producing flexible and adaptive people with the capacity to perform in operations. Operational Evaluations will ensure that our education and learning competency standards are supporting Air Force's joint and network capabilities.

So, for the future, Air Force is centred on success through people. Our Force will always be reliant on highly trained people, both Service and civilian, to deliver extraordinary operational results on the day, while simultaneously planning for and implementing an ambitious, networked, future. The job of the Chief, in partnership with the senior leadership in Air Force, is to make sure those people are well supported and well led. As I said in my introduction, there is no doubt in my mind that the right people in the right culture are central to current and future success.

Turning back to the strategic environment; the new century has not brought peace and stability to our world. Strategic uncertainty pervades. The War on Terror continues—terrorism seems to have become the method of choice for radical ideologues around the globe—and the spread of weapons of mass destruction is still of serious concern.

Violence continues in the Middle East, the reconstruction of Iraq presents a challenge, so does North Korea, and the tension over Taiwan continues to bubble. Internal issues in some nations to our north and east have the potential to translate to external security concerns beyond their borders, such as piracy, transnational crime and refugee flows, and of course, terrorism. Our assistance to East Timor still draws our attention. Internationally, the demand side of state-stabilisation operations seems to be growing, while the supply side—national and international capacity to help remediate problems if invited to do so, or if requested by the United Nations—remains fixed.

This uncertainty poses us, as defence planners, new challenges now and into the future. We, the Australian Defence community, have not been shy of those challenges. We have embraced them. Defence is actively planning its future in concert with our partners in national security. That said, I expect that Defence will continue to

operate in a fiscally constrained environment, and meeting the challenges posed going forward will require some clear thinking, robust risk management and collegiate force prioritisation sustained by open, constructive relationships.

As a start, over the last three years our Chief of the Defence Force has released three seminal documents. They are: *The Australian Approach to Warfare, Force 2020* and the *Future Warfighting Concept*. These documents describe Defence's current and future intent when it comes to warfighting. The shape and balance of our future force will be derived from those intentions, in line with guidance from Government through White Papers and Strategic Updates.

We do not enter the future blindly, nor secretively. These documents are public, so as to provide transparency to the people of Australia, the region and our allies.

Further, the Chief of the Defence Force is about to release the NCW Roadmap. The Roadmap takes the intentions of those seminal documents I just listed and puts a plan around them. The NCW Roadmap provides the direction, and initial steps, to enhance significantly the ADF's warfighting effectiveness through improved collaboration and ability to share situational awareness. It is Defence's internal guide to discovering and exploiting the opportunities of NCW. It is an aspirational document, setting the long-term goals for the ADF's warfighting capabilities through to 2020. The focus of the first iteration of the Roadmap is to detail the initial actions that will set the ADF on the path to an effective NCW capability. Over the next few years, updates to the Roadmap will capture decisions and identify follow-on actions that will improve our capacity to network and so better conduct effects-based operations. This iterative approach will allow Defence to explore the potential of NCW, and how it can be best applied.

The NCW Roadmap lists four key actions that will set the ADF on the road to becoming a seamless, effects-based and networked force. They are as follows:

- **Action 1. Set the NCW-related targets** for Defence to achieve.
- **Action 2. Establish the network** that will link engagement systems with sensor and command and control systems, and provide the underlying information infrastructure upon which the networked force will be developed.
- **Action 3. Explore the human dimensions of the networked force and initiate changes in doctrine, education and training with appropriate support mechanisms.**
- **Action 4. Accelerate the process of change and innovation** through the establishment of a Rapid Prototyping and Development capability in partnership with industry.

In pursuing these actions, we intend to shape our future capabilities to deliver the effects needed to make a decisive difference in the conflict space. Flexibility and adaptability are key systemic traits necessary for success, both as conflict winning attributes and risk mitigators.

Focusing on Air Force, we have to be careful how we balance the evolution of the Force. The Air Force Budget is around four billion Australian dollars annually, which comprises people costs, operating costs, and capital costs.

The cost breakdown is typical of modern enterprises—our Air Force workforce requires about half our budget, so we are constrained in increasing numbers. Operating costs are about a third, and the rest is capital. The Air Force capital budget is supported by the major capital budget—that is, the budget approved by Government for new equipment and systems. Defence’s capital budget limitations mean we have to be very selective in what we buy. The NCW Roadmap will be a useful tool to help us decide in which systems we should invest, and their relative weight as part of a balanced force. Our capacity to make cogent force development decisions will be enhanced by Air Force’s active input into the joint experimentation and rapid prototyping and development initiatives.

Before I talk about our networked future though, I must make the point that the RAAF is already a network-minded force. It always has been. It has been a trait of our Air Force that it could work effectively in a joint environment from its beginning in 1921. And my intention is that we bolster our current joint focus by building an expeditionary, flexible and adaptable Air Force tailored for joint and coalition operations to support the ADF’s networking aspirations and the Government’s requirements.

Let me expand upon this. First, our force must be fully expeditionary. Our structures and systems must support forward operations, whether it is for the Defence of Australia, or for coalition operations further afield. Even Defence of Australia contingencies demand deployments of thousands of kilometres from main operating bases to bare or lesser operating bases in the north. Australia’s famous ‘tyranny of distance’ is both a strategic blessing and a curse. It gives us geographic depth from which to defend our nation but places on us a routine burden for forward operations only a few other nations bear.

Air Force is already a long way down the expeditionary road. We have created Expeditionary Combat Support Squadrons to enable us to deploy to and operate from forward or remote bases, or limited infrastructure operating bases in northern Australia. I expect them to be able to deploy rapidly, establish themselves quickly and launch operations as soon as possible. If we can do this effectively within Australia, we can also do it elsewhere if we retain a flexible, adaptable and responsive approach. We did this in East Timor and the Solomon Islands. We did this in the Gulf at several bases, which, by the way, we continue to support.

Consequently, if you are in the RAAF, you are expected to be available for deployment—ready, equipped, and fully prepared.

Second, Government and coalition partners expect us to provide appropriately tailored and interoperable forces. This could just as easily be to counter a homeland security threat, or the deployment of forces for a coalition as part of a UN mandate, under a regional arrangement, or under a long-standing alliance commitment.

Third, we must be flexible and adaptable to circumstance and the Government's requirements. People and systems must be capable of multi-role employment.

And lastly, if we are to deal effectively with those last three points, we must be networked. You have just heard the Minister talk about Network Centric Warfare and its centrality to ADF capability and operations. I see the Air Force as having a key role in this and, from now, I will refer to my intention as simply 'Networking the Air Force'.

So how do we go about creating the future Air Force? I have already spoken of our strategic focus, our reliance on people as the key to effectively leveraging a network, and our *Learning 2020* initiative. As well, for the emerging Air Force of 2010 and beyond, the capabilities of the past must be systematically augmented. All things being equal, that must be done not by becoming much larger than the force of today, but by creating synergies within the ADF and with other security partners by effective networking.

In this regard, we can learn from our involvement in the Iraq war. What are the lessons from the current Iraq experience that we can translate into future capability for the RAAF? No doubt there are many, and we are still examining and reviewing air power's performance, but I wish to highlight a few standout trends to illustrate where I am coming from.

First is the flexibility our air power brought to the battle, noting that air superiority was established from the outset. Our F/A-18s were dual use systems—they could be quickly switched from air-to-air roles to air-to-ground roles, sometimes in the same mission, to meet any immediate threat or provide a rapid response to meet the Joint Commander's requirements. Tankers were critical. Without them, none of the Coalition could have operated over Iraq. Back home in Australia, we need tankers to overcome the tyranny of distance for transit and strike, and to increase on-station times for supported platforms. We will need to continue to invest in flexible, high-end systems to allow Government a range of options. Examples are the procurement of systems such as airborne early warning and control and the Vigilaire command and control infrastructure which will allow us to network:

- our fighter and strike systems;
- our tankers;
- our intelligence, surveillance and reconnaissance unmanned aerial vehicles;
- our surface assets, such the Air Warfare Destroyers the Navy is acquiring; and
- our Army ground and air elements; and so on.

Second, in the Gulf our fighters carried only precision weapons—no 'dumb' bombs. In the latest Gulf War up to 70 per cent of the total munitions dropped were precision guided as opposed to only eight per cent in the first Gulf War. We have come a long way in ten years. In addition, many of these modern weapons were not hampered by smoke, dust storms or cloud cover. Nearly all tanks and artillery sitting in the open

were destroyed from the air. In this vein, we look to further developing our precision and stand-off weapons for all our combat aircraft. Ultimately, NCW will allow the near real-time target-selection and acquisition needed to deal with mobile threats. I might add that dumb bombs are also operationally viable and cost-effective in particular scenarios, and should not be written out of the analysis yet, if ever.

Third was the value of intelligence, surveillance and reconnaissance that allowed the Coalition to ‘see’ the battlefield real-time, in all weather, night and day. That meant that the Iraqi regime and their fielded forces were pinned down. Every time they made a move they were hit, even, for example, during a dust storm in which they were attempting to hide. All of this shows that we are on the right track in Australia with the further development of systems, such as JORN and P-3, and investment in many new capabilities like Wedgetail, unmanned aerial vehicles and Vigilaire. Again, we will network all these systems to gain even greater benefits.

My final point from the Iraq experience is the value of electronic warfare self-protection equipment. We have fitted such devices to our deployed C-130H and C-130J aircraft, which mitigates the risk to them when operating in a high-threat environment rife with surface-to-air missiles and small arms fire. Electronic warfare self-protection extended their operational envelope, and we are just not effective without it. The broader point is that the days of ADF platforms being ‘fitted for but not with’ operationally essential equipment are passing. And network capabilities are deemed operationally essential for our next generation systems.

Having presented a quick overview of the insights from our Iraq experience, I would like now to turn to our future capability. Our aim is to give Australia the Air Force that it needs for the future; an Air Force ‘fit for purpose’. Air power will remain a major instrument of national power into the 21st century. However, it must remain relevant to both circumstance and means. What we want our Air Force to provide is detailed in the next few paragraphs.

First, a high-end capability must be maintained, regardless of calls from some sectors to radically restructure the ADF for the War on Terror or coalition operations overseas. Our Air Combat Group and Surveillance and Response Group systems shoulder the direct burden of high-end warfighting. These forces are essential for shaping the regional security environment as well as the conduct of offensive operations. The Joint Strike Fighter (JSF), stand-off weapons, unmanned aerial vehicles and the multi-mission aircraft that will replace the P-3 come in here.

The modern way of war and other high-end security operations demand air superiority to permit effective land and sea force manoeuvre. That is an historically proven fact that has never changed since air power emerged in the first half of the 20th century, and will not change in the future. Our joint force elements have come to expect air superiority as a precondition for combat operations. However, we must not take the establishment and maintenance of air superiority as a given, nor presume that the US and others will always provide it. At some time in the future we may have to fight hard to establish control of the air from within our own capability base. And, if we go offshore to fight in our neighbourhood, we will need to control the air, not only over our deployed forces, but also over our lines of communication and over our mounting bases.

We must have a balance between the reality of the present and strategic uncertainty of the future. That means the capacity to extend either a helping hand or to punch hard and accurately. That is why JSF—the first true fifth-generation fighter combining stealth, precision and lethality—will be so important to Australia’s future security.

The JSF will provide a capability that will help us deliver our network centric vision. It will be part of a balanced air combat, strike and close air support capability. That capability will comprise not just air combat aircraft but airborne early warning and control, air-to-air refuelling aircraft, unmanned aerial vehicles, the planned multi-mission aircraft and critical command and control elements. All of this will be part of a realised networked ADF. The capability engendered by JSF and its supporting elements will be expeditionary, flexible and sustainable.

Second, we must have expeditionary enabling forces able to provide mobility and combat air base support—this is where Air Lift Group and Combat Support Group come to the fore. We are already examining future lift requirements in concert with the Defence Science and Technology Organisation (DSTO), Army and Navy, and it may be that we look towards a faster, wide-body airlifter in the future. Networking our support actors is also essential for success, as they are often the first forces fielded in Operations Other Than War.

Third, we must be able to package the force to suit the campaign. For example, during Operation *Relex*, the border protection task in the air-sea gap to our north, we activated our bare base at Learmonth in Western Australia with an Expeditionary Combat Support Squadron to operate four P-3Cs on task. In future, some of these surveillance tasks, including land surveillance, will be flown by unmanned aerial vehicles (UAVs), such as Global Hawk, and we are now looking at how best to support that type of capability.

Finally, and the key point of my presentation today, we need to network all our systems to enhance our combat power. I believe the Air Force to be in a prime position to take the lead on this concept, especially given the emerging capabilities in the pipeline.

So as you can see, the Air Force is changing with the strategic environment. Further, through experimentation and rapid prototyping as part of the NCW Roadmap, the Air Force aims to enhance its capacity to pre-adapt to and better shape the security environment. In playing our part in meeting Australia’s strategic ends, the Air Force will take a hard look at how to refine our culture, our capability requirements, and our concepts for operations.

In practice, how might a networked force operate? I want you to consider a highly skilled, deployable Air Force of the future. Let me paint a picture using an imaginary joint, networked, force deployment in perhaps 2015.

In response to an emergency situation, the Government directs the ADF to respond in support of a host nation who has asked for assistance. Navy, Army and Air Force elements are individually deployed but, through their NCW systems, link as a seamless force. The force is carefully designed, built, and skilled for integrated, networked operations that make today’s joint operations seem clumsy in comparison.

All of the actors—air, land and sea—are using the same operational picture, with their view of the conflict-space customised to need. Strategic, operational and tactical level data is fed into the information grid via a multilevel security system that ensures our decision-makers, operators and support people get what they need, but cannot be easily compromised. Despite the seeming complexity of the net, command and control is simplified allowing superior decision-making. All understand the intent of the operation as it unfolds, ensuring a focus on the objective, enhancing sustainment, and reducing the possibility of fratricide.

The Air Force deployment is carefully packaged. Our intelligence, surveillance and reconnaissance (ISR) assets have been building a physical and electronic picture of the battlespace. A JSF package, airborne early warning and control, and tankers go in next. The initial action is removing the adversary's command and control and ground-based air defence systems using on-board electronic warfare systems to jam and deceive, and air-launched, long-range stand-off weapons targeted through airborne early warning and control, and unmanned platforms to disable and destroy. JSF continues on to control of the air over the area of operations—it is able to switch from offensive to defensive operations as required.

Once an air perimeter is secured, an Expeditionary Combat Support Squadron moves forward to establish an operating base, and forward force elements deploy. The force has a small footprint in theatre, reducing exposure. Unmanned aerial vehicles based to the rear monitor the area of operations, and report enemy moves while also feeding the fused conflict-space picture. The unmanned aerial vehicles are backed up in theatre by the multi-mission aircraft.

Unmanned aerial vehicles provide persistence. With a pair, we are able to loiter over the area of interest with a selected suite of sensors to give us 24-hour a day continuous coverage.

JSF now maintains air superiority and switches modes quickly to attack ground targets when necessary, using stealth, electronic warfare (EW) and precision weapons to maximum advantage. Auto target cueing and prioritisation between platforms—air, ground and sea—is available for the area of operations, including for targets of opportunity. All in-theatre forces are working off a common, synthesised picture. The Jindalee Over-the-Horizon Radar Network (JORN), airborne early warning and control, the multi-mission aircraft, unmanned aerial vehicles, Special Forces, surface and sub-surface maritime platforms, and allied and commercial space assets link to provide seamless, continuous coverage of the close and broader operational environment, as well as providing essential communications links to support command and control and force sustainment. As well, vital support is being provided by industry and embedded contractors. They are part of the networked logistics structure.

The networked ADF has a tremendous advantage, and that advantage translates across the spectrum of conflict in many other scenarios.

Operationally, the air component will be part of a networked seamless force. The capability and system prioritisation and development of such a force is complex.

Financially, it must be within our means. We are off to a good start, but maintaining a balance is key.

Let me now expand on what we in Air Force see as important in developing concepts for the future.

Strategically, we need to be able to shape, deter and when necessary, respond, all with an effects-based focus. But how can we be sure that our direction is sound?

Simply, we will use experimentation techniques to make as many mistakes as we can in the lab or in field-testing before we proceed with acquisition.

While we have capability plans based largely on current systems, we need to stretch our imagination to develop the Air Force of the future. We have established a cell under my Headquarters in the Air Power Development Centre to deal with our future in concert with the other Services. From the top down, we begin with the following:

- First, **Futures Analysis**. The aim of futures analysis is to imagine a set of future scenarios, out to about 30 years, which challenge our force and our security posture. Some of these scenarios will be developed jointly to support the joint process, some singly to challenge air power options.
- Second, **Concept Development**. From futures analysis we move to concept development. Our futures analysis should tell us where we are relatively weak and strong, and how we have to adapt. From there, we develop concepts, or theories, for testing through experimentation. The concepts can be joint, or air specific. Air specific concepts may be needed to satisfy me that my advice to the Chief of the Defence Force and Government on matters pertaining to air power capability is well-founded. The first Future Air Warfare Concept is currently in production through the Air Power Development Centre. The view taken in the Future Air Warfare Concept is somewhat different to the platform-based approach we have used in the past. Instead, we have based our future views along the lines of capability and effect. Doing so is providing a more appropriate basis for understanding our contribution to the seamless force I mentioned earlier.
- Third, **Experimentation**. Future concepts can only be explored by testing and experimentation. I use experimentation in its broadest sense, and include wargaming, simulation, brainstorming, modelling and so on. I see experimentation as an essential risk mitigation strategy in developing our future force. We have already conducted one experiment this year focused on the future Air Force, and it went well. Experiments can be conducted in simulations, in the lab, or with the real force, resources permitting. Air Force now has a four-year experimentation plan in train to test our concepts in partnership with the other Services and national security actors, to support our decision-making with regard to capability development.
- And finally, **Operations**. Once a concept has been proven through experimentation, it finds its way into doctrine and our operational and training systems.

We have been in the formal experimentation game for only a short time, but our early results are useful. In conducting experiments, we take significant input from Army and Navy—extremely important as we will always fight as a joint team striving for seamless results to produce compelling effects.

So how will we use experimentation in the short term? Some typical questions to be explored might include the following possibilities:

- What does it mean to become a fully networked, expeditionary Air Force and how can we enhance our deployable capabilities?
- Considering our current and planned forces, what are the nodes to focus on to give significant capability improvement? We do not want just to surf waves of progress reactively as they wash over us. We want to seize the future by proactively focusing capability or influencing policy with the intent of turning the tide.
- How do we best package an adaptable force to meet Government needs for the near term and the future?
- If interoperability remains a key imperative, and I believe it will, how in a networked sense do we remain interoperable with our allies and others? How interoperable? Which systems will bear fruit? Which do we retire and what do we invest in that will pay real dividends?
- If we adapt our force packages to provide plug-and-play capabilities with allies and coalition partners, how will that affect our expeditionary Air Force construct? Where is the balance?

And there are many others.

In overview, let me make a few general points germane to Air Force's future.

I do not believe the Air Force needs radical change. Our strategic reasons for being—that is, to control the air, project power through strike, and contribute to force mobility—remain as valid now as they ever have, and will remain so for the future. However, we need to broaden our approach to operations, and improve our relationships to enable superior decision-making, both human and machine.

I caution those who advocate a focus on low-end technology and mass through larger forces as the 'ideal' force structure solution for the ADF. Australia has developed high-end systems with much care over many years for valid strategic reasons, and will continue to need them for the future. As I have said before, balance is essential.

First, I do not believe we can afford much larger forces, with personnel costs consuming nearly half our budget already. Better networking will allow us to better leverage the assets we have.

Second, while high-end systems remain expensive, they are an essential insurance policy—one, we hope never to call upon—but they are critical to the national defence.

Whilst the likelihood of having to use them to secure Australia from direct military attack seems low today, the consequences of not having them may be potentially catastrophic given the strategic uncertainties we face. If abandoned, high-end systems take decades to re-establish, notably from the personnel perspective. Re-establishing a cadre of expert practitioners and the logistic support for high-end systems and sustainable, networked operations is neither trivial nor cheap, even if considering future force structures based on unmanned aerial vehicles. Further, well-designed and networked high-end systems provide for flexible and adaptive operations in peace and war, and provide significant deterrence. Ultimately, Government has broader options for conflict prevention and resolution than a more simple and less capable force provides.

The remaining challenge for leaders across Air Force is to understand the cultural disposition of the organisation and to get the work force to think and act differently about historically proven as well as new and emerging concepts.

So to summarise, my goal is to have a clear understanding of how we as an Air Force will operate in the 2010–2015 time frame and beyond, through tested air and space warfighting concepts, which align with the work being done in the joint arena.

We are in the early stages of a truly networked force. For the near term, we must:

- develop a full suite of future operating concepts to guide Air Force development into the future;
- further enhance our concept-led, experimentation-tested, capability development system;
- further develop the use of space and elaborate on the Air Force's role in space systems operations; and
- finally, and perhaps most importantly, become professional masters of an increasingly networked force.

Some may say that all of that is a big ask, but the Air Force senior leadership team recognises that it will be absolutely critical that we get on top of these issues.

In conclusion, I firmly believe air power will remain a major instrument of national power well into the 21st century and Australia must maximise its potential.

- We will define the future Air Force around its culture, its concepts and its capabilities.
- We need to imbue a culture that enables us to think and act now for the future, a culture that makes things happen rather than just letting things happen. We need to challenge ourselves with open minds as part of a shared endeavour.
- We need to keep the right balance between our ability to contribute jointly in homeland defence, to contribute to the security of the immediate

neighbourhood, and to contribute to global missions to protect our interests or support humanitarian interventions.

- The Air Force must become fully expeditionary as the backbone for any operation, national or offshore. We are already well along that track and recent experience has shown this approach is paying off.
- Air Force must retain high-end networked systems, while recognising the vital importance of sustainment, both materiel and personnel.
- Future air and space concepts must be developed and tested, to ensure relevance and inform capability development.
- The NCW Roadmap will be a vital tool to collaboratively shape effectively networked Air Force, joint and coalition forces.
- And finally, we must bring the right people and good ideas together within a framework of a values-based leadership culture and open learning. That is the key for the Air Force's future.



# **NETWORK CENTRIC WARFARE AND AIR POWER**

**LIEUTENANT GENERAL JOSEPH E. HURD  
(USAF, RETIRED)**

First, let me thank Air Marshal Houston for inviting me to participate in this 2004 Air Power Conference. Looking at the agenda, I think it is going to be a great conference as we all discuss network centric warfare from a lot of different positions. I welcome also the Service Chiefs and the delegates from around the world that are going to participate in this conference and I hope to see inputs from you as we go through today and tomorrow too, and then to the rest of the delegates and conferees here I hope we provide food for thought for you too.

Network centric warfare is a new term and no two people agree that that is a name. It goes from network centric operations to command and control (C2) constellations, to battle management command and control, and if you go outside and find somebody standing out on the street they will have another name for it—if they do not they will invent one. That is going to slow us down for a while until we can finally talk in the same lingo that we have talked in for something like interdiction. I do not go anywhere where people do not understand the term interdiction, or air interdiction, and exactly the target sets that is supposed to take on and so forth, but as long as we talk in different terms, to some degree, we will talk past each other.

I am not a network centric type of person who builds these things. I am going to come at it from an operator's viewpoint. How do I use it once we field this network centric capability and put it in the field? What will it mean to me as a commander or decision-maker in the field? So what is network centric warfare? Is the Internet network centric? It is unclassified, connected to a global information grid and you could call that network centric. Is that network centric information the same as warfare or does network centric warfare incorporate more than that? I think it incorporates more. It is more than just moving information. It is also going to be defused information and, as you will see later, it will provide actual knowledge to the decision-maker, whether he is at the staff level or at the commander level. It is using that knowledge. In fact, I believe that initially our staff will get larger as we move more information but are not able to fuse it so that we have actionable knowledge. We are still going to have to read more and we all still have a 'Commodore 64' mind, and it is going to take more and more people to digest that information.

Is it a new type of warfare doctrine? Does this replace strategy from the past that we have been using, at least in the USAF, for a number of years? I do not think so. I think this is an enabler and it allows us to take and use the data that is out there but do it more efficiently, with higher fidelity and less time. I do not think it is a change in doctrine. We will write it up in doctrine—that is true—but it will be an enabler, not a new type of warfare. Does it replace effects-based operations (EBO), or support EBO? Again, I think it is an enabler; it supports EBO. And EBO by itself, when you take it apart, is not necessarily a new type of warfare. I think we have been doing

EBO for a long time. I go back to ball bearing factories in Germany in World War II. Was that an 'effect' that we were trying to achieve? I think so. I think it is the same thing, but we pay good people today to invent new terms and so we have come up with a new term called EBO. It is not a strategy necessarily, but it is a conceptual way to think and it is beneficial to all of us that we go down this road because it will provide us a better control of our end-states of war than we have previously demonstrated in the past. We can no longer afford to tear up and destroy nations in warfare that we have done in the past. So EBO can prevent us from doing that by looking at both kinetic and non-kinetic, looking at the DIME process of diplomatic, information, military and economic ways to achieve effects without having to destroy physically a point or to achieve an effect via kinetic energy. So EBO is something that we want to embrace. Network centric warfare will help us because EBO is going to demand much more data and much more knowledge of the battlefield; not only the options for courses of action for the Blue Force Commander, but also the courses of action that are available to the Red Force Commander and we want to get inside his time loop so that we can react prior to him executing his courses of action. Is it a battle management system? Again, I do not believe it is. I believe battle management is still going to be done by command and control systems; it is going to be a smarter battle command system, but it still does not replace these existing systems. Network centric warfare will not replace Deployable Joint Command and Control (DJC2), Global Command and Control System (GCCS) or any of those other acronym suites that you want to go through today. It will enable them and make them smarter but it will not replace them, in my opinion.

So what is it? If you think about a typical USAF C2 constellation, what we are trying to do is to take all of the different platforms and systems and integrate them into a single fused piece of information so that the decision-maker at the Combined Air Operations Centre (CAOC) or maybe in the Multi-Sensor Command and Control Aircraft (MC2A) or, today, in the Joint Surveillance and Target Attack Radar System (JSTARS) or the Airborne Warning and Control System (AWACS) aircraft can make a decision and have high confidence that he is making the correct decision and also have high confidence that the target and the ordnance that he is going to commit to that target to generate the effect is, in fact, the right target and the right piece of ordnance. So that is what we are trying to do. We are trying to move the information that all these platforms gather, fuse it and then provide actionable knowledge.

So, the C2 constellation network is going to use the Global Information Grid (GIG) to pass all this information to help us in predictive battlespace awareness (PBA) or intelligence preparation of the battlespace (IPB). It is going to help EBO. It is going to provide voice, data, imagery and video; all of those things are going to be in there. It is going to use the Joint Tactical Radio System (JTRS) and new terms that we have not even thought about before with new acronyms, and I will come back and touch base with some of those. But it is going to provide the warfighter with an expanded information sharing capability. His situational awareness (SA) is going to go extremely high, his information is going to be protected and he is going to be given actionable knowledge, and it is going to increase our combat lethality at the end of the day. This constellation is going to affect everybody—the networks, the warriors, the weapons and the sensors—and it is going to pull us all together so we are one. I believe that the hardest part of this is not in the technology but it is going to be in changing the culture that you and I have grown up with over the years. We resist

change in all our nations, the best I can tell, to the last breath. We hate change but we will have to change. This will require a paradigm change or transformational change if we are going to embrace this. And it is going to take us longer to get through that knothole than all the rest of it put together, in my opinion.

As I said, it is a GIG, it is data link connectivity. Data links are going to play a large part in being able to link all of this data together. JTRS is a new radio; it is a new wave form and it is programmable once you have put it into the airframe. Data interoperability is most important—can I read Army data or Navy data, can I read coalition data and vice versa? Can you come to the war and use the database that I may already have established? We have got to work our way through that and it does not mean that you have to buy my software applications in order to do that. I think that there is a way to do that using your own software applications. ‘Portal Access’ is a new term that is currently floating around; it is like using your Internet Explorer on the Internet. You can use that and open up different things and look at it. All Theatre Battle Management Core Systems (TBMCS), which I know the RAAF uses, are going to a portal access type with the next generation. When that happens that means I no longer have to have TBMCS software at the Squadron Operations building. I can just dial up on the Secret Internet Protocol Router Network (SIPRNET), or whatever net we are on, and look at everything that you are looking at in the Air Operations Centre (AOC), as long as you give me the IP address and a password to do that. It is going to mean that situational awareness (SA) across the commands is going to be very much increased, both horizontally and vertically.

Collaboration is one aspect that I would highlight. In watching *Millennium Challenge* and *Unified Endeavour* series exercises, and Joint Expeditionary Force Experiments (JEFXs) for two terms (02 and 04), I think that collaboration, both horizontally and vertically, is the absolute key to reducing our coordination time for controlling the war that we are in. We have all got to learn to collaborate and we have got to do it in real-time, and it has the absolute greatest potential pay-off of any other thing I see out there today. Unfortunately, at least for the US, we have not decided on one collaboration tool as yet. There are a lot out there—InfoWorkSpace (IWS), Defense Collaboration Tool Suite (DCTS) and four or five more—and we have not made a choice and we need to do so. I think it is politically driven, to some degree, by industry but we need to get on through this. We are at the same place we were in the 1980s, when we had WordPerfect and Microsoft Word within the same unit and you could not coordinate a paper across the base because everybody was on a different system. We need to get past this and then, once we do, everybody needs to get to it because this is going to be the key: collaboration.

Looking to the future, some of the defining capabilities, as I see them out to about 2008, are as follows:

- **Multifunction networks.**
- **Data interoperability.**
- **Portal access** for all the C2 nodes.
- Increased **situational awareness** for the AOC.

- **Blue Force Tracker situational awareness.** As you know, we went to war this time in Operation *Iraqi Freedom* and I think there were 17 different trackers available inside the theatre. We have got to narrow that down to about one tracker so we know everybody is on the screen and we have not dropped somebody off, and then we have a fratricide because of the lack of knowledge.
- **Machine-to-machine interface.** A lot of words are being said on this today. We have got to take the man out of the loop. We can no longer afford 1300 people to run an AOC, like General Moseley had in Operation *Iraqi Freedom*. As Air Marshal Houston said, as our Air Forces all get smaller we are going to have to accommodate a lot of that at the headquarters level because we are not going to have the entry positions to bring on new bodies to staff the overhead. So we have got to use machine-to-machine to replace that.
- **Common Data Links.** You must have attachable data links. We must program to get off the Situational Awareness Data Links (SADLs), Improved Data Modems (IDMs) and the Link-16s, so that we will have only one data link and, at least within our Department of Defense, we have decided ultimately to go to JTRS and I will talk more about that later.

Things after this, 2011 and beyond, include data interoperability through Extensible Markup Language (XML), data tagging, and multilevel security coalition operations. They will come in a second level of capabilities, although we have made some progress in JEFX in the coalition portion in the main experiment during July and August of this year. We took new steps forward and we are going to continue to whittle away with that but it will not be totally achieved in the next couple of years.

**Distributed Common Ground System (DCGS).** DCGS is a global network of fixed and mobile ground processing systems for intelligence, surveillance and reconnaissance (ISR) data collected from multiple sources. The system's primary function is to receive intelligence feeds from all sources at a common ground station where they are processed, stored, correlated, exploited and disseminated to enable time critical targeting. It takes the information that we pull off all the different intelligence sources, whether they be Imagery Intelligence (IMINT), Signals Intelligence (SIGINT), Electronic Intelligence (ELINT) or Measurement and Signature Intelligence (MASINT). Currently, we process that individually in each Service but we are under Department of Defense guidance to make this a joint process—I would say firm guidance: they said, 'You will, or else!' We have finally formed a joint organisation and so all of those are going to be brought down to a single backbone under a DCGS called 10.2. That contract has been awarded and we are starting to do the development work, and that is going to provide us with the joint ability to move all this information, both horizontally and vertically, in order to share and fuse that information. Today, mensuration of target points, geographic locations of targets, so that we can use precision weapons, is a long and painful process—it normally runs around 35 to 40 minutes—and that is much too long if you are trying to go after a time sensitive target, which is going to 'shoot and scoot' in five minutes in some cases. So we have got to do better with that. We had a new one at JEFX 04; its nickname is 'Gridlock'. Gridlock will have the ability to give mensurated targets that will support precision weapons in less than ten seconds. Just think about the reduction in time and the enhanced capability that will provide us because all of us are going to

have precision weapon type ordnance. Then we can take bombers that, in some cases, have got hundreds of precision weapons on them and we will be able to target those. If we were trying to target that same bomber using RainDrop software, we would run out of fuel before we ran out of weapons in most cases.

**Radios.** The radios today—SINCGARS (Single Channel Ground and Airborne Radio System), Link-16, CEC (Cooperative Engagement Capability) and all—will eventually go into a common tactical data link and we are starting to move in that direction. As Air Marshal Houston talked about, we are even going to fuse our weapons platforms; the F-16s and F/A-18s will go into a common joint strike fighter (JSF) in the future. Our radios today are all over the sky and none of them will talk to each other. JTRS is going to be the new one and it has different clusters that will service different types of needs; it is a joint program that has been funded and agreed to inside the US Department of Defense.

**Common Operational Picture (COP).** Today we have a family of interoperable pictures—a common operational picture, a common tactical picture, a single integrated aerospace picture—and everybody is all over the map, and none of them really share data in situational awareness that we need. The COP today is not real-time and normally takes somewhere between ten seconds and ten minutes just to see an air picture. I was in Korea for their yearly *Ulchi Focus Lens (UFL)* exercise and I could sit in the AOC at Osan and see an air picture with three to five seconds latency but if I went to the Marine Headquarters, I could only see one with 15 minutes latency—something is wrong with this picture. We ought to be able to move electronic data faster than that and we have to do it. We must have a common tactical picture that will get us into that three to 48 seconds time frame, which is probably pretty good for making decisions. That does not give you the capability to control like an AWACS aircraft can do in a dynamic air engagement, but it gives you the capability to make decisions. Eventually, in the long term with advanced applications, we may take that down to milliseconds but that is in that 2017 timeframe, so I would not get particularly excited about that coming in the next couple of years.

**Tactical Targeting Network Technology (TTNT).** We have experimented with a lot of new initiatives that are going to put more backbone into network centric warfare. One of these is TTNT and, basically, this the ability to take and increase the pipe size of your Link-16 network, and later JTRS as we incorporate that into this new system, so that you can move more data through the data link networks that we have today. It is IP-based, extremely low latency and very responsive, and it will fit on our low observable aircraft. It is going to be JTRS compatible. It will coexist with Link-16 and it is going to have multiple independent levels of security and, eventually, it will incorporate the weapons data links that we are starting to use or develop today to provide guidance to GPS-type ordnance after it leaves your aircraft. All of that will fit inside this. We experimented with it recently. It was a very, very positive experimentation and the final report will include the go-ahead for us to take and field this in the future as we go forward.

**Multi-Platform Common Data Link (MP-CDL).** I would now like to talk about MP-CDL and how it will relate to JTRS and TTNT. Basically, over the last couple of years, using experimentation and doing a lot of analysis, we have decided that we need two different sizes of pipes when you are starting to work in this network centric

warfare. One size is tied primarily to the sensors. So you have Guardrail to AWACS to Global Hawk to U-2 to Rivet Joint (RC-135), down to your ships and down to the CAOC and so forth. We need a large pipe to move IMINT pictures and a large amount of data so that we can increase the fidelity for the decision-makers that are trying to decide what should be targeted and so forth. We have experimented with that pipe and it needs to have a capacity of 45 to 274 megabytes per second, which is extremely large compared to where we are today. Once you make that decision though to put it down to the aircraft and the people that will do the execution, then you will go back to the TTNT/Link-16, which will still have a size of two to ten megabytes. We believe that is the kind of technology that we are going to as we incorporate our ability to do high fidelity network centric warfare into the future. So this is going to affect you, Air Marshal Houston, as you buy your new AWACS. You are going to need a large platform pipe, because that is going to have to incorporate into this and that is where we will be moving that data. It also has to have a Link-16 so that, when it is providing targeting, all we have to push is the target coordinates into the aircraft or to the fighter or the shooter. It has got to have both capabilities. This system has been really successful and I think if we decided that it is what we want, we could probably start fielding it in less than two years in some form, and I think you will see the USAF try to move out on that.

**Joint Tactical Radio System (JTRS).** I talked about JTRS earlier. JTRS is a box and on some aircraft it is going to fit inside existing space that is already there. What it does is bring a lot of different capability. Within that one box are programmable wave forms and so in a JTRS Cluster 1 type it will primarily service those targets that are ground centric, or forces that are ground centric or helicopters, and they will be programmed to fit that particular one. Cluster 2 focuses on handheld radios. Cluster 3 aims more at our large fixed wing aircraft or the large sensor aircraft and in the down links to the fixed targets in the AOCs and so forth, and allows us to communicate with them. Cluster 4 then is the one that really goes to the fighters and the shooters and the bombers for implementation or the execution portion. And then Cluster 5 is primarily built around the hand packs and the handheld man packs, maybe the Special Operations Forces (SOF) as you think about them today. All of that capability can be in the one box and all of it can be programmable. It really gives us the first interoperability across the joint world of the Army, the Navy and the Air Force. It also gives us the potential to work best with coalition assets too as we get into that. Again, it is not hardwired, it is going to be easy to change and so if I need more than one I can organise that on a given day.

**Advanced Tactical Targeting Technology (AT3).** AT3 is a USAF/USN joint program. It is being developed under an Advanced Control Technology Demonstration (ACTD) program and it is the USAF's number one ACTD for FY-04. What does it give us the capability of doing? It gives us the capability to locate surface-to-air missiles (SAMs) precisely and very quickly. Say, for example, you have a lead F-16 flying out somewhere and he gets radar energy on him from a mobile SAM (an SA-6, SA-13 or something like that). Using his own digital threat receiver—the Radar Attack and Warning System (RAWS) gear in our aircraft—he will now transmit information on Link-16 to all the other players about the type of signal that he has received and the specific RF energy to look for in that signal, because each one is just a little different. All the other receivers will then automatically cue to that. As they are all in different locations, you can solve the triangulation problem. What we

can get then is a 50 metre CEP at a 50 nautical mile stand-off, well before the engagement range of some of those short-range SAMs, and you can do it without a combined package of EA-6Bs, Rivet Joint and JSTARS, and all of those other packaging assets that you would have to use today. You could do this just with the engagement package going to the target, and you can do all that within ten seconds. That is kind of remarkable that we can do this. We had extremely good luck in doing this in JEFX 04. Once you do that, the lead F-16 out there could theoretically then fire a HARM (High-Speed Anti-Radiation Missile) at the target radar. A HARM, as you know, is a suppression type munition; it does not necessarily kill that radar van (unless he leaves his radar on and it attracts right to that) but it will force him to turn his radar off. Everybody else now has a precision location within 50 metres and they can go in and do a DEAD profile on it, a destruction of the enemy air defences, and so you get a permanent kill then and not a suppression for 12 hours or 24 hours or even for an hour if he turns his radar off and the HARM misses. There is a lot of capability there; a lot of high potential pay-off because you do not have to 'package' in that medium threat environment. You are able to sustain operations and reduce the risk of where you can afford to fly. Again, it is nothing really new. If you own a digital receiver and a Link-16 you can get into this network pretty easy as we go forward. We think that is really a particularly large pay-off for us.

**MC2A (Multi-Sensor Command and Control Aircraft).** E-10 is the designation that we will give to the MC2A in the future. It comes out with really two missions. One is to act as a sensor and it has got a new radar on it that is called the Multi-Platform Radar Technology Insertion Program (MP-RTIP). It is basically an upgrade to the JSTARS radar that we have today. It is going to allow us to have a better and a quicker and wider area search for ground MTI (Moving Target Indicator) imagery. It will also give us an airborne MTI, particularly for cruise missiles, and gives us the capability to track those missiles and be able to target them en route too. So in a sensor capacity it will do that. It will also give us a capability with an increased Synthetic Aperture Radar (SAR) mode and an enhanced MTI to be able to identify those mobile targets that we see without having to use another sensor, such as a Predator or a U-2 or a Global Hawk, to go take a picture of where that dot is located and say that is a T72 tank or that is a Scud TEL (transporter, erector, launcher) or whatever. We should be able to do some of that on the platform itself, just using the logarithms built into it, and say that is a hostile enemy versus a friendly vehicle that we have got a target location on. So that is the sensor portion that comes with the E-10 MC2A, and then with that is going to be a command and control or a battle management control mission.

**E-10 MC2A Battle Management Control.** The E-10 will give us, within the one aircraft, the capability to go forward in the initial stages of combat and carry all levels of command and control needed, before you have time to deploy an AOC and set up command and control for execution. For example, you could have the Joint Force Commander (JFC) on board, with a control cell that can provide his directions as to what can be engaged and what cannot be engaged and so forth. You also could have all the component commanders on board—the Joint Force Land Component Commander (JFLCC), the Joint Force Maritime Component Commander (JFMCC), the Joint Force Special Operations Component Commander (JFSOCC) and the Joint Force Air Component Commander (JFACC) all on the aircraft. All would have the ability to fly on the same aircraft and interact and do the command and control

forward. Now, once you have established your theatre and you deploy those forces, then the aircraft could be reconfigured because all of it is open architecture and you could pull some off if you wanted to and expand the capability to do more control or keep just the JFACC, for example, if that is what you wanted to do. So it is all open architecture with the ability to be reconfigured up and down the aircraft to make any console serve any of the different functional component commanders and at the same time you can actually do fusion of intelligence information because in the JFACC you have got the AOC execution function—that is the people that are doing the execution of that 24 hour Air Tasking Order (ATO) that we typically use to run our operations—and at the same time you have got ISR management, so they could re-task assets and keep ISR dynamically as new threats pop up. You could cross-link that and re-task a Predator, say, to go right for 20 miles and identify something or task a U-2 to take a different picture than it was originally scheduled to take, based on the evolving threats that you see. You also could control unmanned aerial vehicles (UAVs) so, instead of reaching back to fly that platform, you would actually be able to fly it off the back of the E-10 if we carry that all the way through. At the same time then, you have got air and surface MTI, which gives you the same thing as JSTARS does today, except in higher fidelity, and it gives you that battle management control. So all of that is incorporated and could be used all up and down or can be shared with all the other components. Again, this aircraft will not be seen in the near term—it is probably a 2010 to 2012 timeframe—but most of the package is already under contract. The airframe is under contract, the radar is under contract and there is a solicitation from the USAF on a contract for the battle management and control portion of that, as we speak.

**Network Centric Collaborative Targeting (NCCT).** What we are basically trying to do here is again to use a wide-band, high-speed machine-to-machine interface to cross-coordinate a sensor pick-up from, say, an MTI to a Rivet Joint or to a Nimrod or to a U-2, but to do it in real-time so that we can geographically locate that target precisely, with the location being precise enough that we can employ precision weapons on it without any further refinement. So the key is wide-band, machine-to-machine and the ability to move that back and forth just in the airborne network that is there and then, eventually, you could link that down to a CAOC or something else using some of the other nodes that we already have, such as MP-CDL and so forth. Again, we experimented with that and the results were good. It is just a refinement, but it is really a wider band or a quicker, real-time cross-linking of all those networks in the air than we have ever done before. We have done it mostly by voice before and the real pay-off here is the machine-to-machine interface that we are looking for.

Within our Air Force we are very good at developing hardware and building new things, but we are not very good at trying to teach the people how to use them. We are now big on developing a concept of operations (CONOPS) for what we need first and then building the hardware, not building the hardware first and then figuring out how to use it as we have done in the past, but that is still not the answer. The ultimate answer is to be able to take this decision quality information that you have at the operator level, whether that is sitting in a JSTARS today or whether that is in a CAOC, and get it over to the operator who is going to execute that with that same decision quality information. That is a long path and it is not exactly simple because we do not have it all wired together and it is not seamless at this particular time. We actually built an Advanced Control Technology Demonstration (ACTD) program that

allowed us to go and experiment with this and the first generation of that came out this year. What we are trying to do is meld brain-to-brain at the extremes. In developing these tactics, techniques and procedures (TTP), it should allow us then to make this transition of knowledge over to the shooter so that he could be able to execute that with the same understanding and the same quality of data that we have back at the decision-making level.

**Joint Techniques, Tactics and Procedures.** Today, all of the manuals that the USAF uses are 3-1 series, the USN uses JTTPs (Joint Tactics, Techniques and Procedures), the US Marine Corps does also, but the Army uses Field Manuals. We need to pull all these together into a joint JTTP so that we are all working off the same tactics, techniques and procedures, and we understand how to deploy, regardless of whether I go to US Central Command (CENTCOM) theatre or I go to the Korean theatre. If I do that today, I go to both of them and I use different procedures in both of them, and if I deploy from the States it takes me some time to understand how they are going to war versus the one that I just trained for in Operation *Iraqi Freedom*. We have got to reduce that time and get that taken down and replaced with standards that we use around the world. We have made a lot of progress with this. We have got the human in the loop here with this one and now we are able to take and not only give that high quality data, but also give a confidence factor to the pilot so that he has a high confidence that the target we are assigning him is, in fact, the right target and he is not going to drop a bomb on one that is going to result in a fratricide or large collateral damage or whatever—all those ‘no-noes’ that we never want to get into. This is our first time to get into this type of standardisation but I tell you it is a high pay-off, because as a Service we have not done a very good job of that in the past.

**The AOC as a Weapons System.** You will have heard that systems and platforms like F/A-18s and F-16s and M1A tanks are all called weapons systems, and that has all been defined at the tactical level of war. Where AOCs work and components work is at the operational level of war and we have never called them a weapons system. It has been ad hoc, it has never been trained and it has never had defined training requirements and so forth. The USAF has elected to make the AOC a weapons system and so, when you do that, then you have to treat it like a weapons system and, more importantly, you have to manage it like a weapons system, and the most important thing is you must train it like a weapons system. So now, just like you do block upgrades on F/A-18s, F-16s or large aircraft, we will do block upgrades and manage it so that all of our weapons systems are upgraded simultaneously and, therefore, the training and everything will be the same regardless of which theatre you are fighting in. So where are we today? We are actually today doing a Block 10.1 as a baseline and we have two AOCs that are baselined now: one at Al-Udeid Air Base (AUAB) in Qatar and one in Korea at the Hardened Tactical Air Control Center (HTACC) facility. We would like to bring three or four more up to 10.1 and we will do that by the end of 2005 and then we will have a solid baseline. That baseline has basically got 81 different applications in software and links and nodes that support what is defined as a 10.1 baseline. We will then start an upgrade in 2006 to 2008 to a Block 10.2.

**Strategy and Assessment.** The only tools we give people today to develop strategy in the AOC are Microsoft Word, Microsoft PowerPoint and Microsoft Excel spreadsheet. These are not exactly strategy development tools. You would like to be able to provide more fidelity to do course of action development, course of action

analysis and then selection, so that you understand the course that you pick has a high probability of being effective to accomplish the mission and, at the same time, not have loss rates that are not affordable by us during that execution. So we played with that during JEFX. We found some functionality that we think is probable, but we have elected not to field it because it was not user friendly and requires further development—that is a spiral development process. Air Marshal Houston talked about experimentation in spiral development. We absolutely believe that is the way to go because technology is turning over so fast that if you go off and write a program to solve something in five years, when you finally field it nobody will use it because they are into the next generation already. So, bite off little chunks, field that and spiral it every year and continue to improve it, and that is what we are going to do. We just elected not to field the first one.

**Airspace Management.** We are at the tip of the iceberg on airspace management. Most of the software that we use today, at least within the USAF—the Army has some better—gives two-dimensional displays and we have got to go to three-dimensional displays and maybe even four, because as you integrate the stand-off weapons that are coming in the future and you integrate all the different UAVs from the brigade level all the way up to corps level and all that the Air Force and Navy have got and then you bring in the Navy with their extended range armament that they are buying, we have got to have a better way to deconflict all of this. This is just the tip of the iceberg and it could become our Achilles heel. The key for us to be able to employ all of this within a given airspace is our ability to deconflict this, because if we do not do it, and do it right, we will end up with fratricide and most of us will not be able to support that or support it for very long. So if we want to be able to simultaneously employ our joint fires, we have got to address this and that is going to be one of the big tasks that we take on.

**Information Management.** One of the things that we see in the AOC of today is that we build an information management home page. Everyone is organised differently and, after about four days, nobody can find anything that we have stored on there. So we have got to standardise this. Why doesn't CENTCOM's information management home page look exactly like Korea's home page so that I know exactly where to go if I am an airman or if I am an Army person or whatever, and the data is the same? The only reason we do not do it is a manhood issue between the two different commands—I thought of it first and I am obviously right. Well, we must get past that. This is not a manhood issue; this is an issue of fighting for our nation and doing it right. But again we have not done it and we have got to get past that to an IP-based network more like the Internet.

**Predictive Battlespace Awareness (PBA).** This is a term that we, the Air Force, coined. What we would like to do is use my Chief's expression: General Jumper has said 'I have so few ISR assets that I can't afford to look where the target can't be. I've got understand the battlefield and put those "soda straws" of those ISR assets that I have in a place where there is a high probability there is going to be a target. I can't just go out and gander over the countryside hoping somebody drives through my soda straw so I can go kill it.' So PBA will do that but we are a long time from doing it. We tried to play with it in JEFX but we did not come out with the tool we want. This is a technology issue that is going to take a couple of years, in my mind at least, for us

to solve. A lot of the other parts of network centric warfare will not take as long, but this one will take a couple of years to solve.

**Improved Coalition.** Again, we have got to get to the point where you can come and join the coalition no matter where you are from. There are really two issues here. The one issue that most of us have always talked about is multilevel security and I think that can be achieved and I even have hope now after working with it for ten years or so that we may achieve it in the next couple of years to some degree. That is not necessarily going to solve our problem because you as an individual nation are going to bring your own C2 applications to the war and I must be able to incorporate those and be able to let you use them but look at the data that is inside the coalition database itself, which is already standardised. This is the point I come back to; we have got to have a standard architecture. We have got to agree upon some tools to manage that, using the same language and so forth, because tomorrow's world versus, say, TBMCS today for the RAAF (which is a tightly integrated system of applications and databases) will be more of a loosely coupled system, where we do not talk to the database direct but we will talk to an information service layer above that, and if you can come in and you have got the same standards it will be just like the Internet. If we can make the Internet work around the world, why can we not do the same thing for the departments of the militaries around the world? I mean, it appears to me that it would be simpler, except for this manhood issue. Then you can use your own application. You come in and I give you the right address and I give you the password and you are in, if we all agree on this service layer interface and how to do that. I think that is where we need to go to achieve the second part of this, because just multilevel security will not be the final answer. If I bring you in and give you a complete new application and say you are in and the multilevel security will take care of that part, then you are going to spend three weeks trying to figure out what this application in front of you on the picture screen is telling you to do and how you can read situational awareness off that.

So that is a summary then of where we are today. The Air Force is committed to doing this co-development, more so than I have ever seen in the past. We are looking for joint effects and we are trying to do this in a joint environment. I have never seen the Air Force, Navy and the Army work closer in a development of reducing stovepipes and becoming joint than I am seeing today. At the same time there is a tremendous amount of interest being put on the coalition aspect of doing the same thing, being able to incorporate the coalition, whose partners are unknown for the next engagement until that engagement comes but we have got to be extremely flexible. We know, in all probability at least, that we will not go to a unified engagement again; it is always going to be a coalition of some number but that number may be indeterminable.

**Interoperability.** So for the RAAF what I look at is interoperable data. Coalitions have got to adopt a common network, I talked about that already. There are software tool kits that we publish out of the Electronic Systems Center at Hanscom Air Force Base that tell you the standard service layer that you want to interface with and what you need to write in, and give guidance on XML, data tagging and so on. Portal access I have talked about. I think as the RAAF gets TBMCS 1.1.3, as we field that, that is going to solve your problem, but the rest of the nations need to think about being able to use Internet Explorer and a portal connectivity.

Connected communications and beyond line of sight have to be addressable for all the warriors, weapons and sensors. Air Marshal Houston, there is one that you might want to look at and that is Multi-Platform Common Data Link (MP-CDL)—it is a wide pipe, it is a big pipe. You are already programmed to get your Link-16 and that is going to take care of that and you might start looking at the interoperable collaboration tools that are needed.

**Training.** I have not talked about it and nobody that I see except for myself talks about training. If you do not train, all your other money is ten per cent on the dollar. We do not train yet but we are attempting to correct this problem. So you have got to stand up to training. General Moseley fought with 1300 people in his AOC and I am absolutely convinced 100 per cent—bet my pay cheque on it—that if all of those people were trained to a high level proficiency, he could have fought the same war with 700 people, and some of them would have played golf every other day. That is what I believe training brings to this. Training we have got to stand up to. It is going to cost too because you have got to buy the modelling and the simulations that can create the environment that stresses the AOC just like war and that is not cheap, but it is cheap on the dollar. And it is for sure a lot better than buying all this stuff that I just talked about and using it at the ten per cent level.

So with that, sir, I have almost used up my question time but I will take whatever questions I can.

\*\*\*\*\*

## ***DISCUSSION***

*Mr David McIlroy (Air Force Scientific Adviser – Defence Science and Technology Organisation):* That was a very stimulating address and I thank you for that. I just wanted to comment, perhaps, on one aspect of your CAOC development cycle. I was quite surprised to see that agent-based decision aids were not seen as coming in until 2010 or 2011. I think from the work that we're doing in Australia, which obviously includes leveraging off any existing US activity and, in fact, perhaps ahead of it in some cases, we can be quite confident that these sorts of decision aids would be in advance of that time scale.

*Lieutenant General Hurd:* I think that you're probably right. I would only tell you for sure that the only thing that's in concrete is fielding 10.1, which is the current block, and that everything else over my period of the last six to eight years watching this changes every year. So if the new technology that you talked about is being worked there and it becomes 'low hanging fruit', so to say, and we can incorporate that, then you will see something else drop out of 10.2 and you'll see that move into that. I just showed you the chart itself, and that's where the Aerospace Command, Control, Intelligence, Surveillance and Reconnaissance (AC2ISR) Center believes today that it is going to come, but I have never seen anything like this last more than a year and it gets revalidated every year. So as things become available they tend to move forward and others drop back.

*Mr Peter von Bertouch (Macdonald Technologies International):* General, with these systems that we require for all this network centric interoperability, obviously they are developing very quickly, especially in the US, and here we are, a smaller country, trying to keep abreast of some of those developments so that we can be interoperable in the future. But we're actually chasing developments quite quickly and often the standards, which eventually define these evolving technologies, are actually behind the systems that are being put into operation with the US forces. How can we as a nation define our interoperability requirements by just specifying the international and emerging standards? Do we need to specify which actual systems we want to talk to when we get these systems fielded, rather than leave it up to the tenderers to interpret the standards, which actually may be behind the actual systems we want to talk to?

*Lieutenant General Hurd:* That is a good question because I'm not sure the United States has a handle on this either. When you get into this software type in some of the development we're talking about, you're talking about technology that turns over every 18 months. Therefore, a great idea today, 18 months from now by the time you can field it, may not even be a requirement; we may be well past that within the technology. The best answer that I can give you is that you've got to endorse a spiral development type process so that you bite off smaller chunks on which you can do the research and development and the fielding in a very short time, and then spiral that to the next level. I would never, ever, ever go off and try again to develop something like TBMCS over five years before I fielded it. I mean, when we fielded 10.0, nobody wanted it because everybody had built their own home-grown program because we didn't have the right program out there and getting them to transition was almost impossible. So we've got to throw away our big appetites and try to develop what we can field rapidly. It may not be 18 months in all cases. JTRS, which is a lot of hardware, is not an 18 months spiral cycle, but the software inside there is. I think we have adopted that in the US Department of Defense—the Air Force, I know, has—and that's the only suggestion I can give to you. I understand the politics of developing things within your own country to use your own industry, and I'm not against that, but I think we've got to come back and look at the software standards that we're using, the language that we're developing and the ability to talk to the service layer that I mentioned, and if you develop to that, I am pretty confident in the future we can get to the point through loose coupling that we can take your application and make it part of the coalition at the time of the event. That is probably the best answer I can give you on that.



# **NETWORK CENTRIC WARFARE PERSPECTIVES FROM THE UNITED KINGDOM<sup>1</sup>**

**AIR VICE-MARSHAL IAIN MCNICOLL,  
CBE, BSC, FRAES, RAF**

## **INTRODUCTION**

Is there something distinctive about the UK view of Network Enabled Capability (NEC); and is there a difference between NEC and NCW? This paper seeks to explain what the UK position is and how this position has evolved from our understanding of the strategic context in which UK armed forces will operate in future. The concept that underpins the future employment of military force is briefly described; this leads to an analysis of the equipment issues at the heart of networking and to the importance of understanding the balance that must be struck between the ability to communicate and the ability to act. Next, the vital contribution of people to this new capability is explored, with reference to the other lines of development that must come to fruition. A large part of the introduction of such a capability is ensuring a common understanding and the UK is working on a 'unified message' for the armed forces and the wider Defence community. The operational benefits of NEC are described, but accompanying these are some new vulnerabilities and requirements. Finally, there is a short description of how far down this road the UK is and of where the obstacles lie.

## **UK VIEW ON NEC**

In July this year, our Secretary of State for Defence, Geoff Hoon, presented the second part of a Defence White Paper to Parliament entitled 'Delivering Security in a Changing World – Future Capabilities' (the first part was published in December 2003). In his statement to the House of Commons, he said there would be '... a new emphasis on effects and outcomes, and on the exploitation of the opportunities presented by new technologies and Network Enabled Capability'. The White Paper describes what the UK means by NEC. It is about the coherent integration of sensors, decision-makers and weapon systems along with support capabilities. NEC will enable us to operate more effectively in the future strategic environment through more efficient sharing and exploitation of information, within the UK armed forces and with our coalition partners. This, in turn, will lead to better situational awareness, enabling the application of the right military capabilities at the right time to achieve the desired military effect. But the enhancement to our capability is about more than equipment; accompanying the technological changes will be transformation to doctrine and training, and to how we command and control our forces.

Much of this matches precisely what the US and others are describing as Network Centric Warfare and we should not make too much of the distinction with NEC. Yet

---

<sup>1</sup> This paper is subject to Crown copyright protection.

the UK view places an emphasis on networks enabling these changes, not on the network being the centre of effort in itself. In particular, the UK approach emphasises the importance of the human dimension—in doctrine, training and education, and command and control structures and processes—and that the network should be the servant of how we wish to operate, not the master. A further distinction is that NEC is intended to fulfil commanders' needs in peace, and peace support operations, as well as in warfighting. Our understanding stems from our analysis of the future strategic context and from operational experience.

## **THE STRATEGIC CONTEXT**

The Joint Doctrine and Concepts Centre (JDCC)<sup>2</sup> has studied the strategic context across seven dimensions (physical, social, science and technology, economic, legal, political and military). This work is continually being refined and improved, and is publicly available at [www.jdcc-strategictrends.org](http://www.jdcc-strategictrends.org); an update is in progress for the end of this year, in order to feed into the next biennial UK Defence Strategic Guidance (the principal internal Ministry of Defence policy direction).

Many specific trends are very relevant to NEC. For example, in the Science and Technology dimension, Trend 5 states 'the increases in speed, connectivity, and pervasiveness of information, and communications technology will continue unabated, requiring continual adaptation by UK defence systems ... the command system as a whole will remain a key force multiplier and advantage ...' However, the major summary risk, which of course applies to all and not just to the UK, is that 'the strategic environment will change faster than the UK can acquire and/or apply resources to meet that threat'.

In the first part of the UK's White Paper, this general work on the strategic context was turned into policy, building on the successful Strategic Defence Review (SDR) of 1998, and the SDR New Chapter (dealing with the post-9/11 threat from global terrorism) in July 2002. In the New Chapter, the term Network Centric Capability was used in the context of the military counter to global terrorism, but by December last year, we were clear about what NEC should deliver in broad terms and, as mentioned above, in July this year we have been even more specific.

## **CONCEPTUAL UNDERPINNING**

The UK's conceptual underpinning stems from the UK Joint Vision, published in June 2001, and particularly from the JDCC's major piece of work on the High Level Operational Concept (HLOC), approved by the Chiefs of Staff in February this year. Joint Vision recognises that 'the development of a Joint Operational Picture (JOP) will be of paramount importance and the total intelligence, surveillance and reconnaissance (ISR) package must be responsive and reactive to help enable the high tempo operational impact needed to overwhelm the enemy in deep and close operations'. Joint Vision included specific capabilities that would be required, for

---

<sup>2</sup> The Joint Doctrine and Concepts Centre was formed in 1999, following a requirement stated in the UK's Strategic Defence Review of 1998. It is charged with being a centre of excellence in developing joint doctrine and a future joint vision for the UK's Armed Forces. Air Vice-Marshal McNicoll is the second Director General and has been in the post since June 2002.

example: ‘integrated, real-time, 24-hour capable operational ISR; a JOP; sufficient and secure bandwidth; automation of the selection, identification and prioritisation of targets and their matching to networked joint fires’. But the idea of NEC was not then mature enough to link this coherently into a top-level concept.

HLOC, in contrast, now gives a very detailed view of how the UK wishes to operate in the medium to long term. It does so through an analysis of the Defence Capability Framework: Operate, Command, Inform, Prepare, Project, Protect and Sustain. For NEC, the crucial elements lie in Operate, Command and Inform. But before looking at these in more detail, it is worth emphasising that—reflecting the major risk of the strategic context—the notion of ‘agility’ is at the heart of the HLOC. To quote from HLOC:

Agility is essentially a human-centric attribute, epitomised by the enduring ability of our people to think creatively, to be resourceful and imaginative and to adapt with versatility to the unexpected. However it also has a strong physical dimension. Therefore operational agility will embrace personnel, structures, equipment and procedure. At its heart are four attributes for which we will equip and structure: responsiveness, robustness, flexibility and adaptability, all of which will underpin future individual and collective training. Agility is an instinctive quality in organisations that share information efficiently and which empower their subordinates.

The Operate core concept is: ‘an agile, task-oriented joint force with freedom of action to synchronise effects throughout the battlespace and with maximum potential to exploit fleeting opportunities’. This develops the UK’s manoeuvrist approach, optimising its four functions of Shape, Attack, Protect and Exploit. This will be achieved through a network-wide expression of command intent and a degree of shared situational awareness that promotes much better tempo and freedom of manoeuvre. At present, commanders expend considerable effort coordinating or deconflicting force elements, most often by procedural planning. Fleeting opportunities pass unnoticed or prove too difficult to pursue. A network that provides shared situational awareness will reduce to a minimum this need for procedural deconfliction. NEC also offers an opportunity to reconfigure the structure of our forces and to change the way in which we fight, generating fighting power that is currently latent at the seams between Service components and military functions. Joint fires and time sensitive targeting are emerging examples of mechanisms that can unlock this latent fighting power. To do so requires battlespace resolution that is much higher than currently available, throughout the seven strategic dimensions, and not just in the physical domain. However, aware that resolution will be variable and seldom perfect, we must build flexibility into our way of operating, so that we are not constrained only to being able to operate where we have a ‘perfect’ view. The use of re-configurable, cross-component agile mission groups is an important expression of this agility. They could be widely dispersed in the battlespace, masking intent, and only merge at the point of action to achieve the mass required for overwhelming force and decisive action. Finally, in the Operate concept, it is important to understand the relationship between responsiveness, reach and vulnerability. For kinetic fires, being closer to the target means in general greater responsiveness but increased vulnerability. Maritime, land and air capabilities are characterised by a spread of attributes. For example, in the air environment, strategic air has a permanently high value of responsiveness; the speed and reach of tactical air can make it even more so,

but can suffer from a relative lack of persistence. And both strategic and tactical air may be vulnerable, for example to modern SAM systems. A network allows operations to be conducted with regard to these factors across the components, maximising strengths and minimising weaknesses.

For Command, we envisage Mission Command relevant to the information age, through a network-wide expression of command intent and an adaptive command and control (C2) process. Although the UK believes that our command philosophy is robust, we perceive an urgent need—and the means—to change control mechanisms. Better communication leads to the temptation to over-control; conversely, when communications fail, an over-dependence on technology can be exposed. So the UK doctrine of Mission Command<sup>3</sup> needs to endure, and the network will allow the commander to communicate his intent more clearly and to a greater part of his forces than before. However, the commander will need to be aware, especially in coalition operations, of the cultural differences that can cause intent to be misinterpreted, and a combination of personal contact and network interaction will be required to minimise this risk. Control should then be reduced to the minimum, with the commander exerting only a light touch on the tiller; tempo will be increased as subordinates are empowered to grasp the fleeting opportunities without reference to higher command, but secure that higher command is aware of what is happening.

The Inform concept is, in summary, ‘decision superiority through shared situational awareness within task-orientated communities of interest that exploit collaborative processes in a single information domain’. This relatively simple idea conceals considerable complexity. First, shared situational awareness is not just about having the same data, it will require a common understanding of the operational context and the prevailing situation and imperatives; it therefore is a human construct and is the result of an interaction between information and personal attributes. The collaborative processes require an iterative exchange of information that progressively adds value and deepens the understanding of participants. ‘Chat rooms’ are a limited example of the sort of tool that is required. The idea of communities of interest recognises that not all force elements can—or should—have access to all information. But the network also needs to be rapidly re-configurable to allow unexpected links to be formed for specific purposes. Finally, the single information domain is the most testing of all ideas, not for technological but for cultural reasons, both national and international. The key to unlocking this conundrum is twofold: first, we must drive to ensure that security barriers only exist where absolutely necessary and are not just the result of bureaucratic inertia; and secondly, we need to be able to apply restrictions only to information within the network, and not to access to the networks, by tagging and encryption that is now technically possible.

---

<sup>3</sup> Mission Command has the following key elements: first, a commander ensures that his subordinates understand his intentions, their own missions, and the strategic, operational and tactical context; second, subordinates are told what effect they are to achieve and the reason why it is necessary; third, subordinates are allocated sufficient resources to carry out their missions; fourth, a commander uses a minimum of control so as not to limit unnecessarily his subordinate’s freedom of action; and finally, subordinates decide for themselves how best to achieve their missions.

## **BALANCE OF INVESTMENT – NETWORK/PLATFORMS**

The UK, in common with most countries, is resource-constrained in Defence. Indeed, despite increases in real terms in our Defence budget, adjustments downwards to front-line force levels continue to be necessary. Some of the reasons are well-known: the above-inflation increases in the cost of high technology defence equipment programs (and, of course, in labour costs); and the specific cost growth in some so-called legacy programs, such as the *Astute* class submarine and the Nimrod MRA4. Others are more subtle, such as the assumptions made in the UK's Strategic Defence Review on future efficiency savings proving challenging, and the apparently endemic mismatch between policy aspirations for commitments (and hence overall force structure) and the resources allocated. This background of very taut finances in the UK makes it especially difficult to achieve the transformational switch to NEC.

There is no doubt, especially in the land environment, that 'quantity has a quality all of its own' and the future context will always require numbers of troops. A similar argument supports the numbers of platforms required in the maritime and air environments; this is especially true for sea forces where transit times of days and weeks means that the smaller the force, the less it can be located optimally for all contingencies. Balanced against that pressure is the agility that networks will give to mass forces where desired more quickly. This plays particularly to the strengths of air power, where rapid transit times allow very good responsiveness. In addition, of course, improvements in the networking of forces, and advances in precision, mean that increased effect can be generated by fewer platforms. So we need to come to a judgement on how much to invest in networks at the expense of some decrease in platform numbers, when the pressure on platform numbers is already downwards for financial reasons.

This balancing act does not have a 'right' answer, but the UK has made its position clear. There will be a reduction in platform numbers, even beyond that required anyway by financial pressure, to give the headroom to make improvements to the information infrastructure. The balance of cost-effectiveness has shifted in a fundamental way from sheer numbers towards efficiency of desired impact, achieved by a combination of networking, precision and new concepts and doctrine. This has impacted most noticeably on the RAF and the RN.

## **THE EQUIPMENT FOCUS**

The challenge with equipment is always to map out a migration path from 'now' to the—possibly utopian—future. For NEC, we view this as a three-stage process: Initial, Transitional and Mature. The Initial NEC state in about 2007 is characterised by improved connectivity provided by currently planned equipment. During this period there will be large-scale changes in UK CIS and ISR capability (notably in our introduction of Skynet 5, Falcon, Cormorant and Bowman, and of Watchkeeper and Astor). The Transitional NEC state in about 2015 is characterised by improved integration, which will require intervention in programmed equipment capability to ensure that delivered systems exploit information. Systems such as Typhoon, Type 45 Destroyer, Medium Weight land equipment, and carrier strike, will therefore have improvements to the 'NEC fraction'. The aspirational Mature state in 2020–2030 (delivering the HLOC) will be characterised by synchronisation, delivered by an

equipment program which inherently delivers ‘net ready’ platforms and systems. Of course NEC, as with all transformation, is a journey not an end-state and we recognise that, as technology and our understanding of NEC change over time, we are unlikely ever to reach a fully mature state. Rather, we shall move from one transitional state to the next. The whole approach has considerable implications for UK’s ‘Smart Procurement’, since the cycle time for seeking, fielding and refreshing solutions must become shorter.

Our view of current and planned connectivity between headquarters and major platforms is provided by the NEC Equipment Roadmap. This is an operational line diagram that exposes the connectivity of major systems, but does not show tactical groupings. The mapping needs to be extended to include the important crosscutting, functional communities such as logistics, air defence, CBRN and networked fires. In order to assure coherence across a wide equipment program, the Ministry of Defence (MOD) intends to adopt an architectural framework approach evolved from the US DoDAF, known as the MODAF.

The achievement of NEC will also require continued development of information management techniques, ranging from low-level data fusion and signal processing, through inference and expert systems, to intelligent agent technologies and the means to engineer effective human-computer interfaces capable of providing the rich environment that promotes effective user interaction.

## **THE HUMAN DIMENSION**

Yet none of the changes above will work effectively if our people are not appropriately prepared to exploit the new opportunities offered by NEC. Part of the issue lies in designing appropriate man-machine interfaces and software that assists information flow and decision-making. These more technical aspects of human factors are increasingly well understood, although there is much still to be done.

However, the ‘softer’ factors are generally not well considered. In any crisis, commanders will need the ability to understand, based in part on their experience and intuition, a chaotic, possibly non-linear, battlespace. In fact, commanders will not only need to understand, but they must be comfortable in such an environment. The risk is that commanders will be deluged with information; where in the past there was frequently a paucity of data and therefore a need to find out more in order to make sense of events, in future too much information may allow multiple possible interpretations. The commander must therefore experience this environment in training and develop the ability to recognise patterns that give indications of the future, allowing him to make sense of events and therefore to make sound decisions. For the subordinates, it will be increasingly important to interact in the information domain, to aid in the evolution of complex plans and to contribute to the decision-making process. They, too, must be trained in this function.

The UK is devising relevant training and education programs, which are covered below, but such training should not be restricted to single nations, since the complexity of such human interaction increases geometrically with the number of countries involved in a coalition. The UK is therefore keen to support multinational experimentation, and training, that touches on the human factors associated with

operating in the networked environment. The ongoing US-led Multinational Experiment (MNE) series is a good example of what is required.

## **OTHER LINES OF DEVELOPMENT**

The UK has formed a NEC one-star steering group to draw together the acquisition and development of NEC-related programs. It is chaired by our Director of Command and Battlespace Management and it monitors progress through a comprehensive NEC action plan, which defines tasks within each of the lines of development.<sup>4</sup> The top-level governance comes from our VCDS and cascades through three-star and two-star groupings. Most of the actions underway have been covered above, but it is important to examine the remaining strands to see how each will need to change and what each can contribute.

Force structures will need to adapt. The changing balance in platforms and networks has been mentioned, but a further adaptation is probably required to allow for the rapid formation and dispersal of smaller task-based teams. This trend towards smaller, more flexible forces is reinforced by the new sort of operations that we envisage and it is being embraced by others: the US Army transformation to a larger number of smaller, more independent brigades is a very relevant example. For air forces, we need to be able to force package in unexpected ways, across the traditional ‘stovepipe’ divides between fast-jet, transport and helicopter elements, and—even more importantly—across the environmental divides. Air integration with land and maritime forces needs to be the norm if ‘agility’ is to mean something.

On processes, the network allows reachback. We already use reachback for a range of activities but, increasingly, we will be able to make use of it to reduce further the in-theatre footprint. This is desirable for increasing speed of deployment (fewer forces to move), reducing the sustainment burden, and for increasing the agility of the force. Of course there will still be a balance to be struck; it is hard to envisage that it will be better for the commander and his key staff to be physically divorced from the realities of the campaign. But they should be comfortable having much more of their supporting staff, for example in the personnel, intelligence and logistics areas, present only ‘virtually’. Video teleconference (VTC) ‘meetings’ have become a standard way of working and, provided participants know each other (an important caveat), are as good as, and less disruptive than, a traditional gathering.

Agile logistic support needs to be developed if ad hoc task groups are to be well supported. This will need logisticians to be in the mind of the commander, through collaborative planning, and almost pre-empting decisions in order to reconfigure support to where it is required. It will also require true asset tracking, with visibility of supplies available to planners and to recipients.

## **SHARED UNDERSTANDING OF NEC – ‘UNIFIED MESSAGE’**

The coherent implementation of NEC demands that those within the Defence community have a shared understanding. The UK is approaching this task on three

---

<sup>4</sup> Structures and Processes, Concepts and Doctrine, Training, Equipment, Sustainment, and Personnel.

fronts. First, a NEC Command and Control (C2) model is being devised. This is a top-level view of force structure information flows in two time scales. The 2010 model is being devised by the Directorate of Command and Battlespace Management (CBM) with JDCC support and is aimed at providing the equipment area lead with more detail to allow coherent procurement. The 2020 model is being devised by JDCC with CBM in support and is more conceptual in nature. It takes the HLOC as its starting point and is intended to give more detail to aid longer-term implementation.

Secondly, a NEC Concept of Operations (CONOPS) is being devised, to raise collective understanding and provide a focus for incremental realisation of NEC within operational and training organisations. Finally, a NEC 'Unified Message' is being prepared, which is essentially version two of an extant equipment area publication, expanded to include details of all lines of development. It should answer the question, 'What does NEC do for me?'

## **THE BENEFITS OF NEC**

From all of the previous sections, many of the benefits of NEC should be apparent, but it is important to draw them out as there are also challenges and we need to be able to take a balanced view. We certainly need to avoid pushing NEC implementation just because it is the current fad.

Above all, NEC should deliver the ability to operate at higher tempo. If the 1990s was the decade when 'precision' came of age, then the 2000s is the decade of 'speed'. NEC fundamentally alters the balance between quantity and quality by enabling forces to be agile and by allowing far greater optimisation of force levels and the essential supporting resources. The nature of command and control, and the relationship between them, is changing. Collaborative planning will generate better effects synchronisation. All of these facets combine to allow decision superiority, operating within the opponent's decision cycle and achieving the doctrinal goal of shattering the enemy's overall cohesion and will to fight, rather than simply destroying his materiel: the manoeuvrist approach.

## **THE CHALLENGES**

So we are very clear about the prize within our grasp, but what are the risks to its attainment? The first and most obvious is the technical challenge of integrating command support and communication systems. Here, our work in such ventures as NITEWorks (a joint MOD-Industry endeavour to research and devise solutions to the practical issues of networking) is reassuring us that this aspect is amenable to effort and funding. More important is resolving the security interface issues, nationally and internationally, of the desired single information domain. Here, it seems that a balanced view of risk/benefit is especially hard to take because of the multiplicity of agencies involved, and the fact that these agencies in the UK are not under MOD control. This challenge, however, must be addressed robustly by the military operators defining a clear and unambiguous requirement and not accepting 'no' for an answer. As indicated earlier, the technical fix—tagging of data—seems to be the way forward for multinational interoperability, but there are likely to be cultural as well as technical issues to be addressed.

Any new system or process brings with it vulnerabilities and of course the security aspect just mentioned is a manifestation of our concerns in this area. Computer systems are vulnerable to network attack and computer network defence must evolve to meet these challenges. Again, however, there is a risk/benefit analysis to be undertaken to ensure that too much credence is not given to the hypothetical capability to exploit vulnerabilities. As importantly, however, we need to be aware of the risk of self-induced network collapse and of the need to have doctrine, organisations and skilled people that can cope with systems failure. Mission Command does, though, empower subordinates to act in the absence of new instructions or information, so provided repair times are short, brief interruptions to service can probably be sustained with little impact.

A different sort of challenge lies in the structures and processes field. If we empower cross-component activity as the norm, do our current component and headquarter structures match this new way of working? Should we be treating the battlespace as just one operating space, rather than imposing historical stovepipes? Even more radically, there may be a case in effects-based operations for integrating actors in the diplomatic, economic and even non-governmental fields with military structures. The UK believes we need to move cautiously before abandoning tried and tested structures and much more thought, analysis and experimentation is required before making changes. The JDCC is organising a UK seminar on 2/3 November 2004 to examine this in more detail.

Other risks have been covered under previous sections, such as developing Mission Command for the information age and de-coupling and devolving control, avoiding information overload causing paralysis, and the use of reachback. In addition the risk of cultural differences leading to misunderstandings during collaborative planning is best mitigated through improved knowledge gained by frequent contact—including face-to-face meetings—amongst potential partners. The current experimentation will need to evolve into regular exercising. These human issues cover such areas as team dynamics and psychology, man-machine interaction, and coercion and deterrence theory, and should not be minimised. There is no doubt that they present at least as great a challenge as the technical issues.

## **UK WORK IN PROGRESS**

The intellectual framework and the underpinning development of ideas are, as set out above, reasonably well advanced. The strategic context is well described and the completion of the UK's HLOC earlier this year has provided the overarching concept for the development of NEC. Likewise the ongoing work on the NEC C2 models and on a NEC CONOPS will provide the necessary level of granularity for detailed implementation. The NEC one-star steering group is maintaining coherence across the lines of development and within the overall CBM Action Plan.<sup>5</sup>

In terms of communication and information systems, the Joint Command and Control Support Strategy (JC2SS) will network the joint, RAF and RN CIS by the end of 2005.

---

<sup>5</sup> The UK's CBM Action Plan contains high-level goals for each element of the defence capability framework. A two-star champion is nominated for each goal: for example DGJDC for 'Command', and Capability Manager (Information Systems) for 'Inform'.

The intention is to develop a common set of applications and the whole network will be hosted on the UK's Defence Information Infrastructure (consisting of a head office and a deployed segment). For operational C2, the UK plans to demonstrate the Initial Operating Capability for its Joint Operational Picture (JOP) in December this year during a major exercise. This will include the first demonstration of the recognised environmental picture, overlaid on the maritime, air and land pictures. The JOP implementation team, based at the UK's Permanent Joint Headquarters, has adopted an incremental approach and from relatively humble beginnings (a series of hyperlinked web pages) the JOP is now turning into a useful command and control tool. The MODAF is undergoing investment appraisal in the process of moving from aspiration to acquisition, but there remain a number of issues to resolve, both in relation to the requirement and to the funding of it. There are, of course, numerous additional actions in every section of the equipment program to ensure that the 'Initial, Transitional and Mature' stages of NEC are achieved.

In the training and education field, a number of initiatives are well advanced. The NEC People and Training Campaign Plan is being put in place. Based on the Unified Message and CONOPS, this has three main parts. First, MOD's Director General of Training and Education's training strategy has been adapted to ensure that all MOD training and education relating to NEC is based on current concepts. Secondly, the Royal Military College of Science (RMCS) is taking the lead on identifying and training for the new skills and competencies demanded by the information age and NEC in particular. Finally, the Defence Academy of the UK is developing a NEC facility for real and virtual training. It will be available for the range of technical courses run by the RMCS, for the Joint Services Command and Staff College and for others on an ad hoc basis.

## **CONCLUSION**

The UK is fully committed to NEC and, although compatible with NCW, sees the distinction as important. The commitment, expressed at the highest level, is rapidly being translated into action through a wide range of activities. Fundamental to ensuring that these activities are coherent is a common view of the future strategic context and of the operating concept to match that environment. The JDCC, through its work in Strategic Trends, Joint Vision and the HLOC, has played the major part in setting out these underpinning ideas. In the equipment area, there is a coherent three-stage program to deliver NEC, taking full account of the balance we see between the network and platforms; this is backed up by work in all the lines of development. Most importantly, the human dimension is being addressed, especially the training and education aspects. Questions remain to be considered in structures and processes, but we see this as an area where a more cautious, incremental approach will avoid radical error. There is work being undertaken to ensure that all within the UK's Defence community have a shared understanding of NEC. We are very clear on the benefits to be gained and of the fundamental shift that NEC enables in the traditional tension between quantity and quality of forces. There are risks to attaining our objective and some of the biggest challenges are cultural rather than technical, notably in security issues and in working in coalitions. But awareness of these and associated mitigating action is well underway. In sum, the UK has a clear view of NEC and a clear strategy for implementing it.

\*\*\*\*\*

## ***DISCUSSION***

*Air Commodore Norman Ashworth (RAAF Ret'd):* Air Marshal in your presentation you used the word ‘vulnerability’ only once. Perhaps I’m showing my age a bit, but in developing the concepts I go back to the question of jamming. It would seem to me that with all these communications systems on which the whole network relies, if someone can find a way of jamming them then you’re in big trouble. I also feel that this is a thing that’s being developed in an era in which the US, UK, Australia, et al have not been challenged militarily by a like-size force, probably since the Cold War period. And perhaps they’re being developed in this same sort of era, looking to the future, where they have military superiority over any likely opponent.

*Air Vice-Marshal McNicoll:* It was perhaps an oversight on my part not to have used vulnerability more than once, because I agree with your first premise, and I think I did say that if you have a network on which you have now come to depend, then you are, indeed, opening up a vulnerability. But it leads on to the second point, which is the asymmetry aspect. Where is our asymmetric advantage? It is in high technology. It is in areas like that. For example, if you take the air environment, it’s hard to imagine—certainly in a US-led coalition, but even without them—on most things that you can envisage that we wouldn’t enjoy a degree of air superiority and that we’d be unlikely to be challenged too much in that. That’s a pretty contentious thing perhaps to say, but I think it’s probably true. However, what it leads to is that our asymmetric vulnerabilities are not in our areas of high-tech supremacy. They’re probably not in the networks. They’re probably not in the air defence fighters or our fighter aircraft. They’re probably in those areas in which the terrorists are already attacking, with sometimes devastating effect. And there’s a question in my mind about how much networks can assist in some of the so-called ‘Global War on Terrorism’. I’m much more sanguine about the vulnerability aspect that you highlighted. I started off by agreeing with you and finished up disagreeing with you, so I hope I’ve covered the ground there.

*Air Commodore Mark Lax (RAAF):* One area we haven’t discussed today is the whole-of-nation or the whole-of-government approach to network centric warfare. I just wonder, with the growing emphasis on homeland defence and the other security agencies which we now see proliferating around the world, how you see NEC or NCW affecting that.

*Air Vice-Marshal McNicoll:* That’s a very good question, which I hope my colleague Group Captain Chris Finn is going to address, in part, when it comes to his time to speak. I didn’t major on the effects-based operations part of it, nor on the cross-government connectivity, but it is an important aspect of all of this. I think if 9/11 and Iraq have done anything for us in the UK, it has made us realise the importance—which we’ve neglected up until now—of getting a network across government that is robust in the same way as we would wish our military communication networks to be. It’s not just the transferring of electronic data between government departments; there’s actually a human interaction and a recognition that it is a joint endeavour.

There are some promising ideas and actions in progress in the UK on this. For example, we are just about to announce a post-conflict reconstruction unit. Our Foreign & Commonwealth Office, our Ministry of Defence and our Department for International Development are putting together a unit to work together and that is actually a first for the three departments. Obviously, we have worked together in the past, and Whitehall in some ways is quite well joined up. But actually recognising that you need to network each other to deal with issues and that you are not just dealing with a military lever, but you dealing with diplomatic, economic and international aid—although we wouldn't see international aid necessarily as a lever that we would apply in a punishing sort of sense—is exactly the direction in which we're heading and there's a close linkage to NEC and effects-based operations and in joined up government.

*Group Captain Steve Duffill (RAF – British High Commission):* We touched on coalition operations and the need for interoperability. Clearly, the United States is spending an enormous amount of money currently in development. General Hurd this morning was optimistic that other nations, perhaps the UK, Australia and some of its other allies, would be in a position in future conflict to operate with the United States. Are you, sir, as optimistic as he that in the future, given the challenges we face, we will be in a position to do so?

*Air Vice-Marshal McNicoll:* Steve, thanks very much for that. By coincidence, I was discussing with Air Marshal Houston at the coffee break exactly that topic. How do we keep up with the US, which applies far greater resources and changes direction with more agility? This is strange because you would think that the larger would be less agile, not more agile, but it definitely has more agility within its process, and we run serious risk of backing the wrong horses. There's a couple of things that we need to do. We need to remain, as we are at present, well engaged with the US to understand what they're doing and, where it's possible to do so and reasonable to do so, to influence for our joint and mutual benefit. We also need to recognise that we're not necessarily going to have all the kit that will enable us to interoperate or integrate completely all the time. We see there being three levels of interoperability coming out. There's the deconfliction aspect, which is what you do with people that actually you can't operate with at all; you have to draw lines on a map and say you stay that side and we will stay the other side. There's interoperability, which at least allows compatible ideas and some element of connectivity and, finally, there's integration, which is where you're genuinely part of a total force. We don't see integration with the US being absolutely possible unless there is an element of donation, if you like, from the US side. And I think the US side is also beginning to recognise that that's an aspect that is required, but I'm sort of talking for the US in part of that answer. But I do think there is a number of things we can do to help ourselves, but there are some things that probably we are going to have to rely on the US to help us form as well.

*Colonel Lester Sutton (Army – Australian Theatre Joint Operations Intelligence Centre):* I am intrigued by your meeting on the 2nd and 3rd of November. Looking at sensor-to-shooter and the future of the operational level of command, I was wondering if you had any thoughts on the operational level of command and how it fits into network centric warfare.

*Air Vice-Marshal McNicoll:* That's a very good question and I suppose if I did know the answer to that we perhaps wouldn't need to be having the seminar on the 2nd and 3rd of November. The UK has just recently completed a review of our national operational level doctrine and we have just rewritten a new joint doctrine publication entitled 'Joint Operations', which describes many aspects of the future concept, because in fact we delivered our high level operational concept in parallel with doing our joint operations doctrine. Because I run the Joint Doctrine and Concepts Centre, it was actually the same people doing the same bit of work, so there is cross-fertilisation, some might say infection, of ideas that moves across it. But you need to be a little bit careful in writing doctrine that you don't leap too far ahead, otherwise your reach exceeds your grasp, if I've got the analogy correct. I think probably my caution that I gave in my presentation is the right one, which is that we need to retain what we know now and what we do increasingly well before we make a major leap into doing something with our components that we might come to regret. We certainly need to remember the other bit that I said as well, which is that we can't make this decision nationally, and I'd certainly welcome attendance from other nations at our seminar; although numbers are restricted, so please don't all come.



# **INTERNATIONAL PANEL**

## **THE VALUE OF NETWORK CENTRIC WARFARE TO AIR POWER**

**AIR MARSHAL SUBHASH BHOJWANI  
(INDIAN AIR FORCE)**

**LIEUTENANT GENERAL DATO' AZIZAN BIN ARIFFIN  
(ROYAL MALAYSIAN AIR FORCE)**

### **AN INDIAN PERSPECTIVE – AIR MARSHAL SUBHASH BHOJWANI**

Chief of Air Force, Air Marshal Houston, distinguished delegates, ladies and gentlemen. I must start by thanking General Hurd for demystifying something about these acronyms and abbreviations related to NCW, of which the USAF is so fond. He mentioned that they probably have a group of people working full-time creating these; I must tell him that we have a couple of guys working full-time trying to decipher what his people produce!

Network centric warfare (NCW) entered the lexicon of the Indian Air Force (IAF) and indeed the Indian Armed Forces a couple of years ago. When I started studying this I found that actually our civilian counterparts have been using net centric businesses for a long time. When you think of the banking system, the network of the railways and the bookings that you do on the airlines, these are all net centric. So air forces, and armed forces in general, actually have been followers in this regard. As far as India is concerned, it has started even later in the day. Although sometimes I must admit that I think that is an advantage, because technology is moving so quickly that if one enters late you actually get a more mature and a more developed concept. Presently, the IAF does not have a well-developed road map or, indeed, an air map for what its network centric warfare will look like. We have set up a small group of people who are going to do this, but they just started a few weeks ago and it is going to take them at least six months to get their ideas straightened. So to that extent, what I am going to be talking about is my own construct based on some of the ideas that the project members have gathered.

The IAF suffers from some peculiar problems, which I think are unique. Our equipment and aircraft originate from a number of sources. We have nine different types of combat aircraft, five different types of transport aircraft and six different types of helicopters, not including the variants, and there are a number of variants. Then there are UAVs and radars, with technical, administrative and logistics problems that are related to this diversity. Usually the standards of equipment from western and eastern sources rarely matches with each other. Even basics such as the measurement standards are different; we have aircraft that measure their speed in knots and height

in feet and others that measure their speed in kilometres per hour and their height in metres. And of course the electronic protocols, wherever they are available, are different and totally incompatible. Even where software is compatible, you will find that the interfaces do not always match; that is to say the hardware does not match, so there is no quick and easy solution. I believe that, for the foreseeable future at least, our equipment will continue to come from diverse sources, so these problems will carry on.

As far as NCW is concerned, we also realise that it is going to take a very large piece of the of capital resources that are available for equipment renewal, and I worry sometimes whether the Indian Armed Forces will ever reach the level of sophistication required for interoperability and be truly characterised as a force that will eventually become capable of network centric warfare. So all this has led to a healthy debate, especially over the last 12 to 18 months; does network centric warfare really give such a great advantage? To what extent should the tenets of network centric warfare be followed? Should it be totally network centric, or should it be equipment dependent or selective? Would there be any disadvantages to going the network centric way?

There are problems of overdependence on networks, which may not always be available to operators, vulnerability of networks and the requirements of training of manpower, problems that have been covered by numerous speakers before me. There is also the requirement to reorient the way that commanders make their decisions and the way their thought processes work. Finally, of course, there is the question of which legacy and non-conforming aircraft and systems need to be upgraded and who is going to provide the technology for all of this.

We have been looking at all these questions and the answers came as follows. Firstly, the answer to the need for network centric warfare was a resounding yes; there were very few qualifications. Timely and relevant information, suitably analysed and suitably shaped, was considered to be of paramount importance in a dynamic conflict situation. Jargon and buzz words became common among the people who used to discuss these kind of things—OODA loops, sensor-to-shooter times, collaboration across platforms, seamlessness and a greater emphasis on the commander's intent, rather than his orders. Secondly, the depth and dimension of our commitment to NCW was considered. We felt that while decision-making was somewhat amenable to total automation, the commander in the loop was the preferred method, at least to start with. Later on, with maturity and with trust building up within the system, we felt that there could be greater independence given to automation, to software making the decisions as well, under certain circumstances. And, of course, we also realised that the security of networks would be as important as the security of voice communications and other data links that we depend on these days.

Given India's size and operational philosophy of fighting wars only on our side of the border, the need would be primarily for static nodes. However, I believe that there would be a need for mobile nodes as well to provide the necessary flexibility to meet unforeseen tactical requirements and redundancy. As things stand, there has been a great deal of emphasis on providing optical fibre networks, wired and wireless networks, and satellite networks where they were required. Indeed, by the end of this year we will have our own Defence satellite up in space. Once all this is done and

ready, we are confident of meeting our international commitments in terms of anti-terrorism, peacekeeping and, under appropriate circumstances, coalition military operations outside the country.

The debate on NCW has also brought out some of the disadvantages of excessive dependence on NCW, which I would like to highlight. One, which I have already mentioned, is that the lack of human intervention in decision-making is viewed with a great deal of suspicion by many. And, of course, there is always the problem of the possibility of information overload. Somebody mentioned that traditional decision-making is 10 per cent information and 90 per cent ‘gut feeling’, and that is what brings out the leadership qualities. It is said NCW will reverse the equation. But I think what is going to happen with NCW is that there is going to be not just 90 per cent of information, but there might just be 150 per cent of information and the commander will be actually unable to make a decision.

Another area of concern is that in an imperfect real world what would be the status of non-network capable platforms and systems, or those that somehow remain outside this wired world? We cannot just throw them away. Thus, 100 per cent network capability would certainly take a long time in our context.

Then there were the technical problems, those of bandwidth. We are going towards an assured capability of two megabytes per second, going onto eight very shortly. But, as you heard from General Hurd, he is talking in the region of 400 megabytes per second; that pipe has got to be very, very large. Where are we going to get it from? I am not so sure that we have the capability at the moment but technology is developing so quickly that I think we might just be able to make it. Finally, there is the need for protecting the network itself against attacks, electronic or physical. Perhaps, a new form of warfare, akin to ECM, called Counter Network Warfare would be around the corner. And just as ECM led to ECCM, so Counter Network Warfare or CNW might lead to CCNW.

Coming to legacy systems, which I mentioned a moment ago, it would be impossible for us to upgrade all the legacy systems; the cost and technical obstacles would be unacceptable. I think we would have to do these selectively and we will have to keep in mind the time and cost consequences. If it cannot be done in the next two or three years, then perhaps it would be better to scrap that particular weapon system or platform and, hopefully, go in for something as a replacement. But then the cost factor would have to be kept in mind.

We have tried some shortcut methods with some limited success, thereby achieving some of the goals. What this means is that if it is not possible to integrate a system in real-time, one can try to do it in next to real-time. For instance, some of our older generation of radars do not have radar data processing (RDP). The solution is to transfer the data manually onto a computer, to be passed down in near real-time to the central processing agency; there would be a gap of 5 to 15 seconds, but it is better than not having that information integrated at all.

But I think that the most difficult legacy system is the human being. Until all data generation capture is totally automated, humans are going to be important in data entry, data assessment and analysis. And of course the commander who has to make

the decisions based on all the information—whether it is moulded, shaped, or comes in its raw form—has to reorient himself to making those decisions in the new paradigm.

With reference to technological support and where it will come from, we found that, as was the case of electronic warfare (EW) several years ago, we were not getting the latest technology and there was a need for creation and sustenance of ECM systems—the entire EW suite—within the country. And I think we have done an admirable job. I think that network centric warfare technical capabilities would also be required to be developed in-country, because these technologies are going to be very sensitive and are unlikely to be freely available, or available with adequate security guarantees. It may surprise you to know that this aspect may turn out to be relatively easy to tackle. The reason being that India has a reasonably healthy defence research and development program, including work on platforms, electronics, information technology (IT) and weapons. There is also a very healthy IT software industry, of which I am sure you are all aware. India has a very broad IT intellectual base—indeed the sanctions that were placed on India a few years ago actually gave an impetus to in-country development of core technologies. All this would, I believe, provide a firm foundation for the creation of the necessary expertise in NCW technologies. Already, we have certain ‘islands of excellence’. The IAF has a fairly sophisticated logistics system that tracks individual aircraft components, or identifies the components which belong to different types of aircraft and have different reference numbers but actually are identical; there is in-house software developed to track missiles flying through space and air defence software to provide commanders with optimised interception solutions. But, as I said, these are ‘islands of excellence’; they are not widespread, nor interconnected yet. In this regard I would like to make mention of the Indian space program. Although a totally civilian enterprise, it does give you an idea of the in-country availability of skills required for this kind of a complex activity, including the linking of units which track these satellites in remote parts of the country and, indeed, overseas as well.

As far as the bandwidth is concerned, I think that for the time being at least we have adequate bandwidth and, indeed, redundancy is available as Defence, Government and the industrial sectors have a number of independent networks, which are complementary and can be switched depending on where the priorities lie.

I believe that the way we need to go forward is not to try and create an entire system in one go. I agree with my colleague from the UK who said that they would like to carry out the development work in three stages. I do not know how many stages the IAF would like to divide its program, but I believe we need to encourage these ‘islands of excellence’, while making sure that the software and hardware architecture allows them to plug into one another in due course of time so that, in a matter of three to five years down the line, they will all become a part of a whole. A review at each stage could ensure that some of the things that have been left out at the edges are brought in. That way the cost will be spread out over a number of years and it will allow systems that are not enabled, or not NCW capable, to be allowed to retire gracefully without investing money and effort in trying to integrate them.

Lastly, I would like to mention our air defence sensors, UAVs and fighter reconnaissance resources, mission planning and video conferencing networks. Some

of these have matured and we are very happy with them because they are working well. We have done exercises using these facilities exclusively and find they work well and result in significant improvements in sensor-to-shooter time frames. To ensure interoperability within the three Services, there is a joint Service working group—an Army, Navy and Air Force IT and NCW team—which has been established to act as a global umbrella organisation which will be responsible for interoperability issues.

So in sum, India's Armed Forces, in particular the IAF, are enhancing the quality and the quantity of network capable platforms, albeit very gradually, and India has embarked seriously on harnessing the force multiplier capabilities of network centric warfare. Aircraft, such as the MiG-21, MiG-27 and Jaguar, are in the process of being upgraded. The Sukoi-30MKI fleet already has an in-built capability. We already have an air-to-air refuelling capability and we will require network centric warfare capabilities if we wish to use the AEW&C aircraft optimally. The capability will also be needed if we are to use precision guided munitions that have a credible stand-off range. I am confident that soon we will be devising our own network enabled strategies and doctrines, despite all the constraints. I am sure that very soon these systems will mature and we will be able to achieve the best that is possible from the system.

Thank you very much for your patient hearing; I will be happy to take questions after my Malaysian colleague speaks.

\*\*\*\*\*

## **A MALAYSIAN PERSPECTIVE – LIEUTENANT GENERAL DATO' AZIZAN**

Chief of Air Force, Air Marshal Houston, distinguished delegates, ladies and gentlemen, first and foremost, I would like to extend my sincere appreciation to you for inviting us over here to take part in this ever challenging forum about air power in the future and the land of network centric warfare (NCW).

I dread two things in life. Firstly, giving presentations after lunch, which is a very tough task to do. Secondly, I dread being the last speaker to talk on the same subject, which is also a tough thing to do. I play a lot of golf and when somebody comes up to me and says, 'What's your handicap?' I say, 'Playing golf!' Now, if anybody here were to ask me what my handicap is, I would say the last two or three speakers that spoke this morning and this afternoon.

Experimental and field operational experiences have proven the value of network centric warfare to Air Forces. I am sure most of you are very knowledgeable about these values and, therefore, what I am going to present this afternoon may not be new to you. Nevertheless, there may be some views from our perspective that could generate some interest for some discussion within this forum. I will cover a little on our perspective on NCW, its significance and value, and finally I will touch on some of the related challenges that we have to consider judiciously for small Air Forces like the RMAF. I feel understanding the challenges is very significant because of the ever

important issue of the limited resources that have to be considered to best suit the air operations of Air Forces like the RMAF. NCW is already accepted in this for defence as an information superiority enabler in our concept of operations. It represents the future in the evolution of military thinking towards IT and its impact on the conduct of operations. Obviously, in the forefront is the US, which is perhaps closest to realising the vision of an all-embracing information network. However, from what I heard from General Hurd this morning, they too are having some problems looking into the future on NCW, so it is a very tough task as far as the Royal Malaysian Air Force is concerned. A small nation like Malaysia cannot benchmark itself against the richer, more developed countries with huge defence budgets. We have to make a more modest approach to develop our NCW capability. The approach, very importantly, has to defer to the scope and scale and limits of the defence operating budget and the country's technological capabilities.

The strong platform-centric construct that we currently have will not allow our NCW concept to start with a network. We cannot start at the top; it has got to be from the bottom. We have to start with the present stand-alone, platform-centric weapons and the command and control sensors and selectively link them together in ways that make operational significance. With regards to military operations, although the Air Force forms a crucial component for fighting the traditional war, the Malaysian nation expects more of our involvement in military operations other than war, which also includes countering asymmetric threats, in particular, terrorism and piracy. The overriding imperative, as far as we are concerned, is to see that the prominent operations other than war also benefit handsomely from the application of NCW. In this respect, the terms which we use should reflect and allow more emphasis on the numerous types of operations other than war and not be inclined towards portraying the traditional warfare construct. In addition, we see NCW as a means for fostering peace and widening of allies. NCW is all about jointness and interoperability. It involves joint and combined operations, more so, when it is related to operations other than war. The more interoperable it becomes the more allies we will have.

I will concentrate my presentation more on network centric **operations** (NCO), rather than network centric **warfare**; it is too big for us when warfare is mentioned. The diagram at Figure 1 shows typically the end-to-end integrated infrastructure or NCO environment for the military.

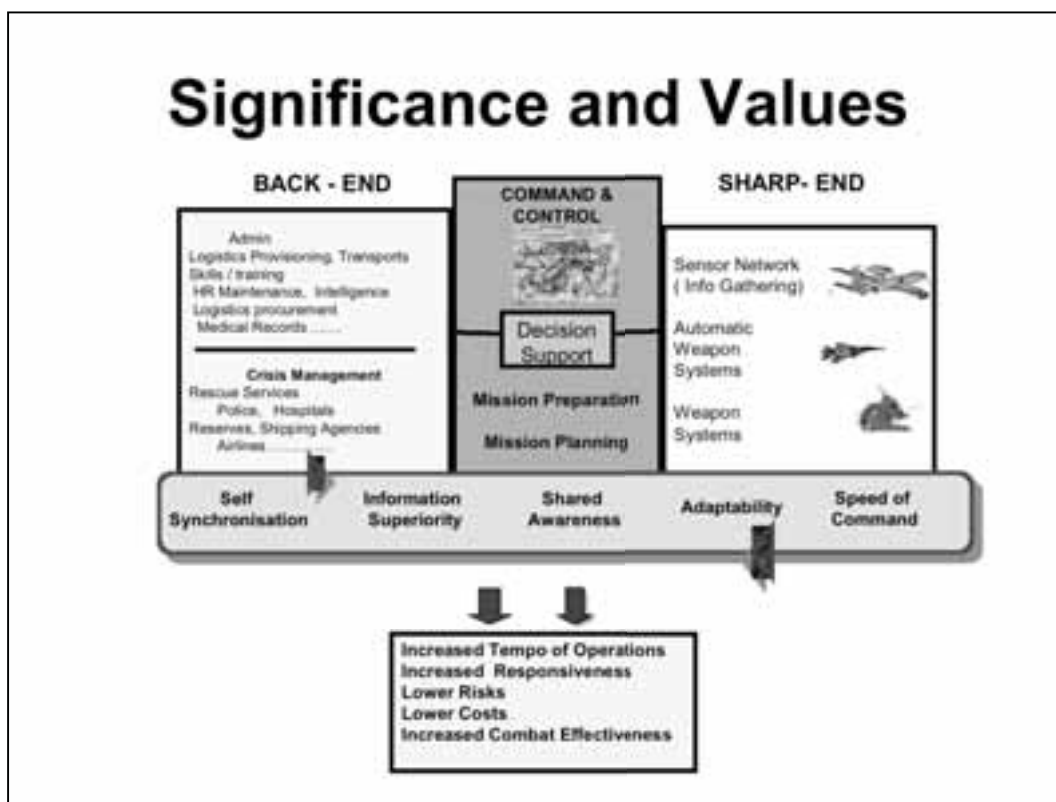


Figure 1 – Integrated Infrastructure or NCO Environment

The infrastructure forms a network that integrates information across all lines of activities. These activities at the back end—as you can see, we are trying at the moment just to improve this aspect of the back end of this whole system—consist of logistics, provisioning, transport, skills training, human resource, intelligence, logistic procurement and crisis management. We want to sharpen this particular area first before we can even go on incrementally into what we have been hearing about this morning and just now. Technology changes by the year and we accept that—by the time we can move into a certain technology, it is going to be changed and we will go back to ground zero again and that is very tough. Of course, the command and control for mission preparation and planning, right through to the ‘sharp end’ is where the lethal and non-lethal weapons systems are employed. This would be the eventual expectation of the Royal Malaysian Air Force towards network centric warfare capabilities.

The consequence to the information flow within the force structure has resulted, as you all know, in the known attributes shown in Figure 1—there is nothing new in this; I am not trying to give you a lecture on known attributes. The aspects of self-synchronisation and shared awareness are essentially the backbone of what network centric warfare is all about. Information superiority offers superior shared situational awareness and when we combine all the grids along and across the board and end to end, it will enable us rapidly and precisely to conduct offensive and defensive operations. Now, having these attributes in place, the benefits are shown as well. I think we all know these: increased tempo of operations, increased responsiveness, lower risk, lower cost and, most important of all, increased combat effectiveness. And as we all know, these benefits do not apply just to traditional war, and my presentation today is about operations other than war (OOTW). Maybe, we can share our

experiences of what we have gone through over the years, something that we have learned ourselves. And the question is, 'If this capability was available way back in the 1940s or the 1950s, wouldn't it have been beautiful?'—wars could have been shortened and less people would have been killed. For operations other than war, speed, accuracy and a common operating picture are absolutely critical in emergency responses, such as responding to natural catastrophes, floods, storms, industrial accidents and even search and rescue. At the present time, the RMAF is more likely to be evaluated on these OOTW-types of operations.

Now a typical response force assembled in a major search and rescue (SAR) or a major disaster in the region will include local and neighbouring country authorities, such as the police, firefighters, SAR teams and so on, and also these components of the military, including the Air Force. Cooperation and interoperability between these responders are critical. The emergency responders or rescuers will require a common operating picture of the disaster area. The command and control centre for the operation will have to have a constant flow of information to and from the disaster area. Communications are vital; specific frequencies to be used need to be known and the protocols for communication have to be there, and transmitting and sharing of GPS data has to take place. All of this must happen. The NCO approach can keep these responders from stumbling over one another and maximise the potential benefits to those involved in these disasters. Simultaneous information flow, a common operating picture and command and search information, and speed of adaptability will enable a more effective on scene response, reduce casualties and provide the ability to compress the overall operation time. Air Force commanders involved in these operations will be able to decrease planning time and also provide flexibility to better manage assets and personnel involved in these operations.

Now the recent search and rescue operation following the ill-fated helicopter crash in Sarawak in Malaysia has shown how critical this information is to us—how critical a common working picture is, how critical adaptability is and speed of command and self-synchronisation. To assist the rescuers in looking for wreckage, special sensors were employed but the search aircraft could not share the images from these sensors. Information had to be relayed through the normal, error-prone voice communications and there was also an instance when a spurious emergency signal from one of the rescue aircraft was mistakenly identified as coming from the wreckage, and the rescuers were sent on a 'wild-goose chase'. All these problems could have been avoided through good, effective NCO capabilities.

For counter-terrorism and insurgency, all countries around the world dealing with these threats will rely more than ever on the network of advanced information technologies that allows them to interpret data smoothly and provides them with vital information. Air power has always been ready to provide capabilities in the areas of dominant manoeuvre and precision engagement that can be leveraged against these adversaries. However, the reality of life on the ground, as illustrated in Iraq, Afghanistan or even in the Philippines, in which terrorists operate in small, dispersed formations, means that air power alone is not that effective when dealing with these terrorists. More foot soldiers are required on the ground. The basic idea is to get these people to become sensors and to relay enemy positions into the network via data links, calling for air support to deliver munitions and precision guided bombs to the targets.

A classic example of what we experienced during the days of the communist emergency in Malaysia was that typical operations were **non-network centric**. We relied heavily on the error-prone voice transmission systems; messages from soldiers on the ground had to be relayed to a field level of command before they were conveyed to the RMAF, which would then provide close air support, medical evacuations or, sometimes, the resettlement of populations into a different area. We would find out that logistical information, weather information and target locations were not near real-time and sometimes distorted. The Air Commander and commanders at multiple levels of ground forces and of commands across two military Services did not have a common operating picture. Control was ineffective and there were instances when different views of reality led to miscommunication between commanders. Mission planning was also time-consuming, required multiple planning iterations and was very ineffective. Time lines to accomplish what we call today John Boyd's OODA Loop (Observe, Orient, Decide and React) were far too long and the RMAF could not accomplish its 'Action' portion, for which it was responsible, with the required speed and accuracy. Now, NCO would enable collaborative mission planning, which would improve synchronisation and reduce deconfliction, and enhance the quality of information and situational awareness from information sharing and collaboration that would compress the time line for the OODA portions of the loop.

In maritime surveillance and counter-piracy, piracy has been on the rise in the waters of South Asia. The RMAF main role in counter-piracy is to conduct surveillance over Malaysian waters. Now this responsibility requires the Air Force to accomplish the two 'O's (ie. Observe, Orient). To achieve this unprecedented, shared information superiority, the Air Force has to be linked at tactical and strategic levels with other government agencies and services and organisations. This has not happened yet. Information will be obtained not only from multiple sensors, human intelligence agents and data bases, but data will also be merged in the future from agencies and forces that have never been linked before. More importantly, data will be transformed into useable information and then quickly distributed. Sightings and information from the Air Force could be rapidly distributed to other Services and agencies to act upon and the net result would be a significant time line compression of the overall OODA look and on the 'sharp end' of the typical diagram that I showed you. The US has conducted special projects on this kind of thing, as was explained by General Hurd this morning, and I do not wish to expand further. In our own context, the kind of a dissimilar combat tactics that we apply on our two very uniquely different systems of the MiG-29s and the F/A-18s are two classic examples of what we see and the report holds true of what the US has done in their report on applying a formation with just radio transmissions against a formation with data link and radio transmission. The bottom line is that we see that aircrews fighting with shared awareness could increase combat power by over 100 per cent. In general, all these situations that I have explained a little just now illustrate how NCO, through shared awareness, helps the Air Force to heighten the pace of operations and coordinate the facts. These speed of command and synchronisation features can combine to create a massing of effects, rather than a massing of forces. That they can be ready to strike effectively without massing forces creates a lot of advantages, which is very important, and being smaller also means a reduction in casualties. NCO will also enable the Air Force and other Service elements and organisations, organised as a single joint network system and

collaboratively planned, to achieve missions far more rapidly and decisively, with greater effect and at less cost than was possible earlier.

Last but not least are the challenges. This to us is a very important area to consider because, with the ever-changing technology that has been described by General Hurd earlier and with the kind of way forward that the Royal Australian Air Force is planning for the year 2020 and so on, it is a concern for us because of the limitations that come with them if you were to undertake these projects in the future. The challenges are in education and transformation of culture. Network centric warfare is relatively new to many developing countries like Malaysia but we are looking to the future and, if the successes of the multimedia super corridor come through, that will be something for us to look at to achieve the kind of NCO capability that we want to have in the future. The challenge is in educating and changing the network itself. The present network, with the present organisation and cultures, makes it more difficult to handle in any kind of operations. These organisations are not only confined to those in the armed forces. We all know that network centric is across the board; it involves the public and private sectors, right up to our political masters. Establishing trust and hope in the viability of NCO in developing countries like Malaysia is a challenge, as the benefits cannot be clearly seen and the possible investment is huge. Establishing trust in the possibility of adapting the technology, as I said, can be a problem. We need research and when you do research you need funds. When you need funds, you have got to develop this trust with the Government because they just want to see what is available and successful. Failure is not acceptable.

Shifting from the present platform-centric system to a network centric system must be done carefully and incrementally, but at the same time we must ensure that we do not fail to take full advantage of what NCO offers. There has to be a lot of experimentation—I would agree with what Air Marshal Houston said this morning—and this may be an iterative process because the experiences of other Air Forces have shown that with NCO things are not always right the first time. That also was supported by General Hurd this morning in his presentation. A sound transformation in reference strategy must be in place so that the process of coevolution takes place as smoothly as possible. In addition, material and systems procurement must not be carried out in isolation, but in accordance with overall NCO requirements. Shifting of platforms, systems and supply of new systems, as well as the setting up of the infrastructure, should as much as possible be sourced from local industries. However, given the level of technology capabilities of Malaysia and perhaps other developing nations, a fair amount of know-how will have to be copied from OEMs (Original Equipment Manufacturers) and the forces of developed countries, such as the US and I see also there would be some avenues with the Royal Australian Air Force. The question is how willing and sincere will the transfer of know-how be to the recipient and how much will the recipient be capable of absorbing. Perhaps a joint venture approach involving local and established vendors in NCO installation may be the best alternative to begin with. However, a better approach would be to have memorandums of understanding (MOUs) between companies, with the patronage of the Government.

The other challenge is the cost of development. It is high. However, before the question of costs is considered, the challenge is to define a workable network centric solution in terms of scale and scope and capabilities, which accommodates the financial capability of the country.

Now whether in traditional warfare or asymmetric warfare, or the variety of operations other than war, the Air Force has to work with other Services, agencies, government organisations, sometimes in a coalition environment. For this to happen there must be jointness and systems interoperability. To achieve this within the national level will require a new concept of operations, common infrastructure with assured reliability, integrity of the information that passes through and then an integrated approach to shaping not only the armed forces but also the national infrastructure. However, it will be more difficult to achieve this with coalition partners because this will not only require a common concept of operations and compatibility procedures and acumen, but also depend on the willingness to interpret and invest enormously in the system.

In conclusion, how do we feel about this? What has been talked about this morning, this afternoon and probably tomorrow, for us, sounds horrible. General Hurd's talk and the keynote address of your Chief have caused more confusion in my mind about how to go about it now, because these things change every other time. We start off on one foot and try to put in the other foot, but before the other foot cuts in something has changed, and we have got to put the other foot in again and so on; this is tough. As I said, NCO is a relatively new concept for us and it needs nurturing to mature. We clearly see that NCO offers significant value to air forces, big or small. It is the value that it offers that makes the development of network centric operations for the Air Force inevitable. But in embracing the development of high-tech network centric systems, the Air Force has to consider judiciously a host of related challenges. We must consider this very seriously, otherwise precious dollars, time, effort and perhaps life could be unnecessarily wasted.

\*\*\*\*\*

## ***DISCUSSION***

*Air Commodore John Harvey (RAAF – Moderator):* Thanks General, and thank you to both speakers for two excellent presentations that move us along in our discussion. Based on the discussions this morning and this afternoon, we now have five national views on network centric warfare from Australia, the US, the UK, India and Malaysia. I think, as we've seen through the presentations, there are a lot of similarities between all the countries' views and, certainly, up at the level of the philosophy and the concept, there's strong agreement. Once we get down to the implementation, we start noticing the differences between the resources available, the size of the organisations, their expectations or aspirations, and also some cultural differences come out as well, which I'm sure will be a challenge if you try and work together on a network centric basis amongst a broad coalition. We've got a chance now to ask a number of questions. Perhaps, we can start off focusing on questions on the presentations from our guests from India and Malaysia and then we can broaden it to include some comments from our speakers this morning. So I'll open up now for any questions.

*Air Commodore Norman Ashworth (RAAF Ret'd):* Air Marshal Bhojwani, in your opening remarks you made some observations that I think are quite important to

network centric warfare and the understanding of it; they were the comments about the proliferation of acronyms and terms and what have you, and the people that were working both to generate them and to interpret them. It seems to me that one of the problems with network centric warfare we've heard so far today is that this proliferation of terms, which the military seems to love, has really got out of hand almost. And I think it's got out of hand to the extent that we might well not understand what network centric warfare is all about because we get bogged down in the acronyms and we try and think in the terms of the acronyms. I would be interested in your comments on that problem. Are you in India, for example, generating your own set of acronyms or are you going to take some common lot, or are you going to throw them all out?

*Air Marshal Bhojwani:* I totally agree with you because that's what I started with. I think it's important to have acronyms in certain circumstances because each acronym then actually denotes a particular project or a particular concept of operations. To that extent, it's very essential. Unfortunately, where I come from all this has happened so quickly that it's very difficult to keep up with it. But I guess it's essential, because when you look back at the kind of acronyms that have been developed in the last 10 or 15 or even 20 years on various other kinds of operations, and ECM and electronic warfare come to mind very readily, the only difference was that those kinds of acronyms and those kinds of individual concepts of operations were spread out over a period of time and it was relatively easy to absorb it. The problem now is actually the time compression. Indeed, that's what NCW is all about; it's actually going to provide so much information to the commander that he's going to have a problem in keeping up with the various concepts under which those bits and pieces of information are coming up to him. I think it's a form of counter network warfare operations that, perhaps, we'll start creating our own acronyms now and, perhaps, bring the Americans to their knees with our own set of acronyms!

*Squadron Leader Tim Anderson (RAAF – Air Force Headquarters):* Many of us in Australia find it very interesting that you're able to integrate and operate aircraft from both the old Eastern Bloc and Western technologies. Do you think that this is a hurdle towards your development towards NCW enabled capabilities? And also do you think there's anything for the rest of us to learn in terms of interoperability across coalitions in terms of integrating different systems from different areas?

*Air Marshal Bhojwani:* Initially, it was considered a big problem. The French Mirage 2000, for example, doesn't have a 1553 [Mil-Std-1553 bus]; it's got something called a Digibus, so while flight data is being carried through the wires, it doesn't come out in the same manner as the one from the 1553 bus. The Russian system, of course, doesn't have it at all. So what we've done is that we've got interfaces which can modify the Digibus data to make it 1553 compatible. Similarly, the Russian systems have been upgraded now and we are making sure that they are 1553 compatible because, once you have a common standard, then you can use the data, either coming out of the aircraft or going into the aircraft. Initially, there were certain problems, but eventually it did become doable. It's a question of time and cost; there were problems over that. Now, I think it's come to being an irritant, which has to be dealt with and it's not impossible to make these things work.

*Air Commodore Harvey:* I guess an extension of that is if we look at the Internet with a whole range of hardware systems out there but a common standard that allows people to communicate regardless what it's based on.

*Group Captain Ian Farnsworth (RAAF):* A lot of you have talked about information overload. What strategies do you have to cope with prioritisation of information? What tools are available to people to make good decisions with a lot of information?

*Air Marshal Bhojwani:* I'm personally not competent to answer that question because it's technological, but I think most of the information processing must be done at the back end. What comes out to the person who's actually going to take the decision—whether it is the commander sitting at headquarters or at the field level or anybody else in between—the front end will give him only what he needs to know, and should he need to know more, he should know where to go looking around for it. So it depends on how cleverly the software is made and how these various layers work in relation to each other, so that all the information is available on the network but only what you need is actually being displayed at your specific level. That's the way I'd like to see it being done.

*Air Commodore Harvey:* A question for Air Marshal Bhojwani. There have been recent exercises in India with F-15s and Indian aircraft. Have there been any lessons learnt from that for approaches to network centric operations?

*Air Marshal Bhojwani:* Lots from the Indian side but they learnt from us also and I'll tell you why. We spoke to some of the pilots from the United States Air Force and we found that they were depending a lot on situational awareness created by the presence of AWACS and other sensor inputs but, when they came to India to exercise with our aircraft, these inputs were not available to them. So, in fact, they'd got used to flying in a semi-networked environment and they were out of sorts when that environment was taken away. The lesson to be drawn from that is that one mustn't become too dependent on this kind of 100 per cent situational awareness because it's not going to happen every time.

*Air Commodore Peter McDermott (RAAF – Director General Reserves – Air Force):* I would like to address ourselves, perhaps, to the title that's up there in front of us at the moment and I've been thinking about this most of the day. We're speaking in the Royal Australian Air Force about network centric warfare and I hear other people speaking about network enabled warfare. I think back to the last time we had a discussion here and we spoke about transformation of force and before that the revolution in military affairs etc. I wonder whether in ten years time from now we might look back upon NCW and NEW, and say, 'Yes, that was but a means to an end in terms of the development of air power. It was part of the process.' How much of what we are talking about today is part of the process and how much, in your view, is it an enabler?

*Air Marshal Bhojwani:* Once again, I'm not competent to answer the question but I can add to the discussion. While studying the subject I created three terms to understand the whole thing myself. One was 'network capable': meaning, is the device that you're using, whether it's a sensor or a shooter or anything else in between, capable of being plugged in, plug and play if you will? The second is

‘network centric operations’, meaning that when you’ve got all of these sensors and when you’ve got all these engagement technologies available to you and they’re all plugged in, then can it help you make an optimal decision, within a realistic time frame? Can the man in the field or in the air actually carry out the intent of the commander by looking at all the information that’s available on the network, on his screen or on his platform? And lastly, we come to ‘network enabled warfare’, meaning the kind of warfare possible only if you have a network of systems and platforms. In other words, you cannot even think about it, you cannot even conceive such operations unless you have the network in place. Let me give you an example. We had a terrorist situation in the northern part of the country a few months ago and we managed to put up a UAV at about 10,000 or 15,000 feet above the area. The terrorists were holed up in a building, which had a high wall and you couldn’t see over it, you just couldn’t observe what was going on inside. We were able to jury-rig the payload download from the UAV down to the guy who was actually giving orders in the field. We put up a VSAT [Very Small Aperture Terminal] over there and he got streaming video of the view from above in real-time. With the result the commander in the field was actually able to carry out a very successful anti-terrorist operation. Now this kind of operation would have been unthinkable if the concept and hardware of networking had not been available. So, ‘network capable’ for plug and play, ‘network centric operations’ when you have lots of platforms working in unison and ‘network enabled operations’ allowing a revolutionary way of employing the tools of warfare. I think the lexicon is still expanding.

*Major Mal Brick (Army – RAAF Air Movements Training and Development Unit):* Network centric warfare gives commanders the capability to reach down to a far lower level with more information than they’ve ever had before. The British presentation prior to lunch mentioned the importance of directive control. How do you consider the two things or do you see them being mutually exclusive? Do you see commanders being able to resist the temptation to micro-manage as a result of the information they now have access to?

*Air Marshal Bhojwani:* That’s what it’s all about I think; orienting the commanders from a very young age to ensure that they don’t take over. In fact, network centric warfare intends to do exactly the opposite. The Commander makes his intent known and, with trust and understanding between the top-level commander and the commanders at the lower level, the decision-making should be taken at the lowest level of command. But you’re absolutely right, it requires a very mature commander at the top, who has all the information and yet isn’t obligated or forced into taking a decision. He must leave that to the lower levels and yet retain the prerogative of taking over should the need arise. It’s all to do with training. The whole morning we’ve been talking about training the people; the people includes the commanders, I believe.

*Air Commodore Harvey:* Just to expand that thought a little bit. Do you see in some cases, automatically, when the level of activity goes up that it’s just a matter of saturation at the top level; they just can’t dig that far down? Do you think that’s a possibility?

*Air Marshal Bhojwani:* Well, it depends. After all, all of us as senior commanders have actually been through the field and there’s always the tendency to believe ‘I can

do better than or take better decisions than the person lower down', except that it's the person lower down who, I think, has a greater feel for what's going on, despite all the information that's available on the net. That's the important thing that the commander must allow, whether it's one per cent or ten per cent—put any number on it—the gut feeling and the leadership qualities of the men in the field will have to come out, even in a networked situation.



# **NETWORK CENTRIC WARFARE AND THE ADF CRITICISMS AND POTENTIAL PITFALLS**

**PROFESSOR ROSS BABBAGE**

## **INTRODUCTION**

Network centric warfare (NCW) is having a dramatic impact on the ways in which advanced combat operations are being conducted. Moreover, the prospect is that NCW will have an even more dramatic impact during the coming two decades.

Nevertheless, NCW is a contested concept. There are at least twelve major criticisms that have been made of NCW in recent years and it is important for Australian defence planners to consider whether all of these issues have been addressed adequately as their planning proceeds. This paper argues that, in fact, almost all of the potential problems of adopting NCW have been recognised by the Australian Defence Organisation for some time and that current planning is being progressed to take adequate account of most of them.

This does not mean that there are no serious pitfalls ahead for the ADF in this field. There are at least two major, additional dangers that need careful attention. The first is that the ADF may be tempted to focus too strongly on NCW in its own right and miss the opportunities arising from the broader defence transformation agenda. Australian mastery of NCW is very important for the future, but defence planners need to realise that NCW offers just a better *means* of conducting military operations. In order to optimise Australia's military capabilities for the future, other new capability elements need to be developed in parallel. In particular, it is important to ensure that Australia's version of NCW be accompanied by the development of improved ways of identifying priority strategic *ends*.

This paper argues that in order for Australia to develop an optimal approach to its Defence Force modernisation, the country's variant of NCW needs to be developed in close partnership with a new concept of operational strategy that focuses strongly on the achievement of key strategic effects. This combination of NCW and Effects-Based Strategy (EBS) has the potential to be extremely effective in Australia's security environment.

## **WHAT NCW OFFERS AUSTRALIA – IN BRIEF**

NCW is starting to have dramatic effects on the way that most advanced military operations are conducted. In particular, the combination of more effective wide-area surveillance systems linked in near real-time to command centres housing commanders who are authorised to act rapidly is dramatically improving the efficiency, effectiveness and speed of many categories of operation. It is, most notably, delivering comprehensive situational awareness and shared understanding to

those who are connected. This, in turn, provides the potential for decision superiority and intuitive multi-unit coordination. This means that desired effects can be delivered with great speed, at unexpected times and in unexpected places. Rather than sequential and predictable operations, NCW permits simultaneous, parallel operations in depth. If such efforts are well directed, the result can induce shock and paralysis in opponents. Indeed, in many situations, victory can come faster, with fewer casualties and much lower collateral damage.

Australia, hence, has strong incentives to pursue its own version of NCW. Fortunately, NCW is adaptable to most future types of ADF operation. NCW has the potential to help compensate for the small mass of the ADF as it tries to defend 20 per cent of the earth's surface. It also has the potential to help the ADF maintain a qualitative edge in the region. Other incentives to pursue NCW strongly include the fact that it will be essential in order to maintain interoperability with United States forces. Moreover, failing to exploit NCW would appear to carry serious risks, not least in rendering the ADF vulnerable to those countries which do.

## **THE TWELVE SERIOUS CRITICISMS OF NCW – HAS THE ADF GOT THEM COVERED?**

Whilst the attractions of NCW are strong, Australian defence planners need to be mindful of the dozen main criticisms of the concept and ensure that the potential hazards in adopting NCW are avoided. What are these criticisms, and are there appropriate responses readily available?

### ***Criticism 1: NCW Would Not Work Against Near Peer Competitors of the Western Allies***

An obvious problem with this criticism is that there is presently no country, or combination of countries, that can compete in conventional terms with the Western allies. However, if there were one or more peer competitors to confront the Western allies, it is reasonable to ask whether the West would be better off not pursuing NCW. This seems highly improbable.

In addressing this criticism it is also important to remember that NCW is not an end-state—it is really much more of a process. New, smarter elements are continually under development that would further complicate any future peer competitor's chance of competing with the network enabled West—at least in any symmetric manner. In consequence, while there is little room for complacency, NCW exploits many of the West's competitive advantages.

### ***Criticism 2: NCW Has Little Applicability to Operations Other Than War (OOTW)***

The reality is that, largely because NCW and related concepts are making the Western allies exceptionally powerful in conventional military operations, many potential adversaries—especially non-state actors—are being driven to asymmetric responses. However, it is reasonable to ask whether this is a disadvantage of NCW. Forcing potential opponents to abandon conventional battlefields is not all bad news.

Nevertheless, it is certainly the case that not all elements of NCW can be fully utilised in OOTW, particularly when such operations need to be conducted in urban and other forms of dense terrain. However, gaining the greatly improved and widely shared understanding of the battlefield situation that NCW can provide in such situations is much to be preferred to widespread ignorance and unit isolation. In practice, border control, counter-drug, peacekeeping, protected evacuation operations etc, can all gain greatly from the employment of NCW capabilities.

***Criticism 3: The IT Needs of NCW Will Never Win Budget Battles When Competing Against Traditional Military Platforms***

This assertion flies in the face of Australian budgetary experience during the last decade. Even a cursory review of the Australian Defence Capability Plan reveals that IT and related systems *are already* being funded at far higher levels than was the case a decade ago. Certainly it is the case that implementing NCW requires increased levels of IT and related expenditure, but this does not mean that the adoption of NCW would, or should, put an end to expenditure on platforms.

Hence, while there might be a risk of IT failing to receive the priority it deserves from time to time, this assertion underrates the wisdom of Australia's defence decision-makers and that which is implicit in Australia's budgetary processes.

***Criticism 4: Getting Inside the Opponent's Decision Cycle Will Not Necessarily Win the War***

True! There is a need *both* to get inside the opponent's decision cycle *and* have the right strategy. I say more about this later.

It is important for Western campaign planners, in particular, to be careful about the assumptions they make about an opponent's operational time frames. Some opponents (including some terrorist groups) operate within quite different—frequently very extended—time scales. Nevertheless, the ability to operate within the opponent's decision cycle is never a disadvantage.

Hence, getting inside the opponent's decision cycle and having superior knowledge delivers a great advantage, even if it is not always decisive.

***Criticism 5: Information Overload Can Stimulate Hasty and Faulty Decisions***

Whilst this is a risk, appropriate, accurate and timely information sure beats ignorance.

Nevertheless, in order to prevent hasty and faulty decision-making, information flows need careful management. Tailored information processing and display systems, combined with carefully developed decision aids and appropriate training, can largely overcome this potential problem.

The reality is that, contrary to this criticism, tailored and accurate information flows generally facilitate higher quality and more timely decisions.

***Criticism 6: Chasing 100 per cent Theatre Transparency Can Generate a New 'Fog of Systems' and Paralyse Decision-making***

This is also a potential risk, but quality command training is an effective antidote. Moreover, all military staff need to be aware that NCW will never provide 100 per cent theatre transparency and the immediate potential of NCW must not be oversold.

The ideal is for commanders to be well-trained to cope with ambiguity and, indeed, to thrive on it. Chasing the last bit of information is certainly no substitute for timely decision-making.

***Criticism 7: NCW is Vulnerable to Direct or Indirect Attacks on its Information and Communication Systems***

Yes, but this does not make the concept of NCW invalid. The answer is to expect multilevel attacks on the NCW and related systems and build in resilience. If this is done, attacks by opponents will be survivable.

Attacks need to be anticipated in several forms, including:

- physical attacks aimed at the physical destruction of one or more key nodes or facilities,
- electronic attacks aimed at incapacitating one or more systems, and/or
- psychological attacks aimed at encouraging friendly forces to lose their trust in key NCW system(s).

There is clearly a need to be able to make the opponent's subterfuge transparent, to strengthening capacities to look through camouflage and decoys and to minimise friendly force misperceptions by sharpening sensor mixes. There is also a need selectively to harden communications and other key elements of NCW, to build in redundancy and to train all key personnel to cope flexibly with temporary or partial system incapacity.

***Criticism 8: NCW Involves Micro-management and the Second-guessing of Tactical Decisions***

Campaign planning needs to assume that politicians and senior commanders will want to monitor, and sometimes exercise control of, tactical developments. The risks inherent in this 'reach-down' need to be recognised and managed by training and exercising *all* key players, including ministers, regularly.

It is appropriate and important for an NCW system to ensure that senior commanders and politicians always have access to quality information and advice. This is not a new challenge, and if carefully managed and combined with quality training and reasonable experience, can provide great strength and resilience to a national command system.

It is also necessary for all players to appreciate that a quality highly-dispersed NCW campaign will make many corporals (and privates) responsible for almost instant on-the-spot decisions that may carry ‘strategic’ import.

***Criticism 9: NCW Encourages Commanders to Become Lazy and Use ‘Standard’ or Mechanical Approaches***

This is a real danger. It highlights the fact that NCW must entail much more than mechanical sensor-to-shooter target servicing.

The potential for mechanical responses in an NCW system underlines the critical importance of upgrading education and training in parallel with the adoption of NCW. Useful mechanisms include allowing more free play in challenging exercises, permitting more ‘competitive Command Post Exercise’ activities and rewarding those commanders and command teams who excel in generating truly innovative approaches.

***Criticism 10: Information and Networking Cannot Substitute for Combat Manoeuvring and Massing***

This is simply not true. The right information management and knowledge systems *can* substitute, in part, for force manoeuvre and mass. The right NCW systems mean that forces can move securely much faster and in more dispersed modes and, while fires (and other effects) may need to be massed, forces themselves rarely need to be so.

Hence, NCW changes the *types* and the *scales* of manoeuvring and massing that make greatest sense. Getting these new dynamics right is one of the primary creative challenges for those adopting NCW.

***Criticism 11: NCW is Just the Latest Fad. Leave Us Alone So That We Can Focus on Getting the Basics Right***

This suggestion implies that the information revolution will go away if one simply chooses to ignore it. Well, it won’t!

Moreover the logic of this criticism is flawed on other grounds. Yesterday’s ‘basics’ may be far less relevant to battlefield success in the future. Stability might give some people comfort and familiarity, but failure to adapt while the world moves on risks battlefield surprise and disaster.

The best antidote to this ‘leave me alone’ sentiment is realistic combined exercising that demonstrates dramatically the consequences of ignoring NCW. Doing nothing is soon shown to be a good recipe for losing most forms of combat operations.

***Criticism 12: Those Pursuing NCW Fail to Pay Sufficient Attention to the Human Factors in System Change***

This is, in fact, one of the most serious risks in pursuing the NCW path. If human factors are given insufficient attention, not only will most benefits of NCW not be

realised, but many personnel will actively avoid adaptation and even generate unhelpful work-arounds that can cripple an NCW system.

Successful introduction of NCW needs to be accompanied by substantial changes to doctrine, training, exercising, reward mechanisms and much else besides. These dimensions of change need to be carefully planned, explained, 'sold' and even negotiated so that the total system that is implemented works in a cohesive, flexible and sustainable way.

## **THAT'S NOT ALL – THERE ARE TWO OTHER SERIOUS DANGERS**

In Australia's case, it will not be sufficient for defence planners just to focus on overcoming these twelve primary criticisms of NCW. There are at least two other serious risks for Australia in moving rapidly forward to adopt NCW.

### **Risk 1 – NCW as an End Rather Than Just a Means**

The first risk is that Australian defence planners and commanders will perceive NCW to be an *end* in itself, when it is really only a more efficient *means* of achieving higher strategic goals.

Vice Admiral Art Cebrowski, one of the fathers of NCW and the Director of the Office of Force Transformation in the Pentagon, recognised this risk as far back as 1999:

Network-centric warfare is a concept about *means*. To operate in a network-centric environment is not an *objective* or a goal of combat. Likewise, to operate network-centrally is not a *strategy* for conducting combat. Rather, network-centric warfare is a tool, a means to empower strategies to accomplish objectives, or ends. Whatever the question, NCW is neither the answer nor the plan to obtain the answer.<sup>1</sup>

There is a real risk that some Australian defence planners will seek to adopt NCW on its own under the misperception that this entails sufficient modernisation or defence transformation. This would be a serious mistake springing largely from an over-concentration on means rather than ends. This is part of the rationale for some leading strategic thinkers preferring to use the term network *enabled* warfare rather than the term network *centric* warfare.

### **Risk 2 – Adopting NCW in a Strategy-Free Zone**

The adoption of NCW should not conceal the need simultaneously to adopt new operational strategies to make the most of the new means that NCW can provide. It is argued in this paper that a very effective approach for Australia would be to develop a locally designed combination of NCW and Effects-Based Strategy.

---

<sup>1</sup> Vice Admiral Arthur K. Cebrowski, *Network-Centric Warfare: An Emerging Military Response to the Information Age*, Presentation at the 1999 Command and Control Research and Technology Symposium, 29 June 1999, [http://www.nwc.navy.mil/pres/speeches/ccrp2\\_.htm](http://www.nwc.navy.mil/pres/speeches/ccrp2_.htm), p. 1.

What, then, is Effects-Based Strategy? Effects-Based Strategy (EBS) acknowledges that the heart of strategy is the battle of wills between the opposing decision-making elites. EBS planning hence begins by identifying the preferred outcome(s) or positions that one wishes the opposing elite to adopt, both in peace and in crises.

Then, springing from a deep understanding of the opposing elite's culture, attitudes, circumstances, etc, EBS planners select and apply a succession of finely tailored measures that are designed to move the opposing decision-makers to a policy position that one prefers.

In his outstanding recent discussion on the philosophy of effects-based operations, Dr Alan Stephens describes this methodology as one in which:

... the desired effect/outcome of any action, regardless of its scale, should be identified before that action is initiated, and ideally should be complemented by its associated ways and means.<sup>2</sup>

Dr Edward Smith, in his path-breaking book on the subject, defines effects-based operations as a:

... coordinated set of actions directed at shaping the behaviour of friends, foes and neutrals in peace, crisis and war.<sup>3</sup>

How then might EBS and NCW be combined to have such powerful effects in a wide range of circumstances? In order to illustrate the potential it is appropriate to consider the following two hypothetical situations.

### ***Hypothetical 1***

- President Walter of Nangaland has no intention of giving way to the ambitions of General Resta, the leader of the regime in Kamaria. He fiercely resists General Resta's assertion of sovereignty over the disputed strip of seabed until in late June, when he is approached by the Kamarian ambassador. In a private conversation, the ambassador advises President Walter that he has lost effective control of his secret Swiss bank accounts and that his daughter, who is studying in Kamaria, has been taken on a 'protected holiday' to an undisclosed location. He encourages President Walter to contemplate these developments overnight and consider the scope for an honourable and early compromise on the seabed issue.
- When the ambassador departs, Kamarian sensors in the presidential palace and three spies on his staff monitor closely President Walter's reactions. At first, he responds with anger and smashes a decorative platter in his office. However, within an hour he has summoned relevant officials to discuss possible compromise positions on the seabed dispute.

---

<sup>2</sup> Alan Stephens, *The End of Strategy: Effects-Based Operations*, Working Paper No. 383, Strategic and Defence Studies Centre, Australian National University, Canberra, December 2003, p. 1.

<sup>3</sup> Edward A. Smith, *Effects Based Operations: Applying Network Centric Warfare in Peace, Crisis, and War*, Command and Control Research Program (CCRP) Publication Series, Department of Defense, Washington DC, 2002, p. xiv.

- On the following day, the Kamarian ambassador again visits President Walter, armed with a well-developed understanding of President Walter's bottom line. First, the ambassador shows the president a video of his daughter holidaying at a seaside location, and assures him that she is well and in good spirits. Then, in a surprise move, the ambassador tables a proposed approach to resolving the seabed issue that addresses most of President Walter's concerns. What's more, the ambassador suggests a series of steps that would have the effect of making the outcome appear to be a political victory for President Walter within Nangaland. The discussion thence focuses primarily on how to implement these plans and how to best ensure that the benefits of the proposed compromise are fully delivered.
- Two months later, at a carefully choreographed summit meeting, President Walter and General Resta sign a seabed agreement and announce a new era of cooperative development between the two countries. President Walter's daughter flies home the following day and he also receives a coded statement of the balances of his secret Swiss bank accounts.

### ***Hypothetical 2***

- President Kwan Kim refuses to order a cessation of Jaffaland's rapidly developing nuclear weapons program. Despite numerous representations from a range of countries and several United Nations Security Council resolutions, Kim refuses to budge.
- The Prime Minister of Northern Halifax and the President of Calgary, who have long been concerned by Kim's intransigence, decide to bring the issue to a head. These close allies have in recent months been monitoring President Kim's attitudes, policy positions and plans exceptionally closely. However, when they move to communicate directly with Kim, he responds by ordering an escalating series of armed clashes on his border with Calgary and disappears into one of several underground command centres in the mountains.
- In these circumstances, the Prime Minister of Northern Halifax and the President of Calgary agree a plan to pressure Kim to relent by threatening and then attacking the core interests of some of Kim's family members and his closest friends. In early September, two weeks after the start of the crisis, three of Kim's family and eleven of his close associates receive cell phone calls, SMS and e-mail messages advising that their business premises and family holiday houses would be destroyed unless President Kim comes to his senses, halts the border incidents and ceases Jaffaland's nuclear weapons program. Whilst it is not possible to monitor Kim's thinking closely in his underground command centre, there is no discernible change in his position during the following 48 hours.
- The next night, the shoe factory owned by Kim's brother is destroyed by a precision air strike and the holiday houses of two of Kim's close associates are demolished. New cell phone calls remind Kim's associates that their personal assets remain very vulnerable if Jaffaland does not moderate its behaviour. During the following 24 hours, Calgary intelligence detects several of Kim's

associates taking steps to convince Kim to reconsider his position. The following night the seaside retreat of Kim's golfing partner is bombed.

- In mid-September, Kim orders his foreign minister to announce that in a spirit of reconciliation with Calgary and with the international community, the Government of Jaffaland would shortly commence consultations with relevant governments on halting its nuclear weapons programs and opening relevant facilities to international inspection.

Such hypothetical use of EBS might, to many, seem far-fetched and highly improbable. However, a variant of *Hypothetical 2* was, in fact, employed effectively against President Milosevic in Serbia in 1998. In response to his intransigent position in Kosovo, the Western allies first threatened—largely through cell phone calls and other messages—the businesses, holiday houses and other assets of several of Milosevic's close associates. In order to encourage them to twist the President's arm strongly, several of these facilities were destroyed and the result was that Milosevic changed his stance.<sup>4</sup> This so-called 'crony targeting' was shown, in those circumstances, to be effective.

Similarly, prior to and during Operation *Iraqi Freedom*, United States and other allied forces made extensive use of cell phone, e-mail and other messaging to persuade key members of Saddam Hussein's regime and armed forces to refrain from using chemical, biological and radiological weapons.<sup>5</sup> Several key commanders were also reportedly bribed to disobey the regime's orders and many others were persuaded to abandon their posts or redeploy their units in non-threatening ways as allied forces approached. The consequences were far-reaching, leading to the speedy disintegration of most of Saddam Hussein's forces and to the capture of Baghdad within 12 days of the land campaign's launch.

## **SOME OF THE CHALLENGES OF NCW–EBS CAMPAIGN PLANNING**

There are many ways in which an opposing decision-making elite might be influenced to shift its position in a direction that one would favour. Some of these ways are direct and some indirect. Some are very subtle and barely detectable to those not directly involved and others are very blunt and obvious. In most circumstances, the most effective EBS campaign would contain a mix of incentives and threats; that is a mix of 'carrots' and 'sticks'.

We would, however, be wise not to assume that the processes of persuading or coercing an opposing decision-making elite to shift positions to something more compatible with one's interests would be predictable or simple. All social structures of the type we are considering here will be complex adaptive systems that will run on their own cultures, sets of values, interests and internal mechanisms. Understanding in advance the way such decision-making groups will respond to particular external stimuli is fraught with challenges. One would clearly need to possess a very detailed

---

<sup>4</sup> See this reported in, for instance, William Arkin and Robert Windrem, *The Other Kosovo War*, Special to MSNBC, 29 August 2001, <http://www.msnbc.com/news/607032.asp?cp1=1>.

<sup>5</sup> Andrew Krepinevich, *Operation Iraqi Freedom – A First-Blush Assessment*, Center for Strategic and Budgetary Assessments, Washington DC, 2003, pp. 17–18, 32; and Walter J. Boyne, *Operation Iraqi Freedom*, Forge Books, New York, 2003, p. 34.

understanding of the given society's culture, etc. However, that would not be enough. One would also need to be so intimately familiar with the histories and habits of the key personalities and their relationships with each other that one could effectively 'get inside their heads'. When one is advanced in this respect, campaign planners would be in a superior position to evaluate the likely responses of the targeted personalities to a wide menu of operational options. However, even when these processes of evaluation, known as Operational Net Assessments, are conducted with great care and in the light of quality information, they are always hedged about by uncertainty. Leaders, or maybe a key individual in the group, could decide to act in a manner that is not anticipated. This will always be a risk that campaign planning needs to take into account. Various backup steps and operational options would need to be held in readiness should the opposing elite not move in a desired or anticipated direction.

Hence, when preparing and launching an EBS campaign it would clearly be essential to have on-hand extremely knowledgeable and well-informed advisers who can effectively model the more likely responses of the opposing elite in a range of circumstances. It would also be essential to prepare a layered series of options that can be employed at short notice, if required, to coerce an opponent to move in a desired direction if his initial responses are in another, undesired, direction.

Conducting operations with this level of attempted precision would require extraordinary levels of close to real-time intelligence, very high levels of command capacity and exceptional operational flexibility in order to maintain the initiative. Most of these exceptional means are potentially available to Australia through the creative development of NCW. If done well, an EBS-NCW campaign of this nature would appear to have the potential to be exceptionally effective.

A tailored EBS-NCW campaign of this kind would also be very difficult to counter. Were a targeted leadership to decide to change direction markedly, this should be detected very quickly and, were appropriate mechanisms in place, there should be a menu of options 'on the shelf' that could thwart such aberrant behaviour at the strategic, operational and tactical levels. Certainly the EBS-NCW combination would provide a national government with many more options that would be deliverable with far greater precision and in much shorter time frames than would be the case were conventional campaign planning employed.

### **KEY CONSEQUENCE 1: NOT ALL NCW FORCES WILL BE EQUALLY EFFECTIVE**

This discussion makes clear that simply adding NCW to an existing force structure-doctrine mix (that is, an incremental approach) may be very tempting but would be sub-optimal. Whilst such an approach should improve operational efficiency, it is unlikely to produce optimal campaign and strategic outcomes.

Implementing a carefully configured combination of NCW and Effects-Based Strategy should generate far better operational efficiencies, significantly modified force structures and greatly improved theatre and strategic outcomes.

**KEY CONSEQUENCE 2:  
AUSTRALIAN ADOPTION OF A COMBINED NCW–EBS  
DEVELOPMENT PROGRAM WOULD GENERATE SOME NEW  
DEVELOPMENT PRIORITIES**

Adopting a combined NCW–EBS development program would clearly require new emphasis to be placed on some key capabilities, in particular, on:

- Deeply Focused Intelligence;
- Close to Real-Time Communications, Command and Control;
- Special Diplomatic Capacities;
- Sharpened Information Warfare Capabilities;
- Highly Networked Military Capabilities;
- Economic Warfare Capabilities; and
- Whole-of-Nation Security Approaches.

**KEY CONSEQUENCE 3:  
THE POTENTIAL BENEFITS OF A COMBINED NCW–EBS  
DEVELOPMENT PROGRAM ARE SUBSTANTIAL**

This discussion highlights the potential of the NCW–EBS combination to markedly improve the effectiveness of Australia’s campaign and strategic effectiveness assets. In particular, it would offer:

- Directness of effects—because tailored persuasive effects would be aimed precisely at the opposing decision-making elite. This should provide markedly improved effectiveness and efficiency, and the possibility that many crises and conflicts may be curtailed in both length and scale.
- Fewer unwanted collateral effects than other approaches.
- A clear rationale for whole-of-nation planning. After all, a much wider range of national assets would need to be engaged in both the intelligence gathering and in the delivery of effects with precision against the key individuals.
- Potentially deliverable at a lower cost than ‘conventional’ options.
- A degree of strategic clout that may otherwise be unobtainable, not only because of its effectiveness and efficiency but also because it would be very difficult for both state and non-state actors to counter.
- A unique strategic edge because Australia is better placed than most to implement such an approach effectively and gain the full range of benefits.

#### **KEY CONSEQUENCE 4: THERE ARE SOME CLEAR INDICATORS OF THE PATH AHEAD**

Were a decision taken for Australia to pursue the NCW–EBS path, several practical steps could be taken towards implementing such an approach in the short term. They might include:

- appointing a senior (three-star?) officer to manage and coordinate orderly NCW–EBS experimentation, learning and change;
- providing this person with a small staff to design, develop and test promising effects-based leverage packages;
- launching coordinated studies into the implications for:
  - command and control;
  - intelligence priorities, systems and resources;
  - strategic planning employing whole-of-nation resources;
  - Defence Organisation training and education; and
  - Australian defence doctrine, etc;
- using Rapid Prototyping and Development processes to test out new concepts in the field (that is, learn by doing);
- rewarding energetic pursuers of the transformation agenda;
- engaging closest allies in a phased program of NCW–EBS desktop and field experiments; and
- providing a simple means for encouraging the results of NCW–EBS testing and experimentation to exert a strong influence on defence and broader national security capability development.

#### **CONCLUSIONS**

This leads us to the following five key conclusions:

- First, this analysis suggests that an Australian version of NCW would provide greatly improved operational efficiencies.
- Second, most of the standard criticisms of NCW can be managed if defence planners are pro-active and persistent.
- Third, it is important to remember that NCW is just a better tool. NCW should not be an end in itself. Moreover, NCW's value would be limited if it were just bolted onto current structures, systems and doctrines.
- Fourth, NCW on its own is not enough. It needs to be combined with creatively-adapted Effects-Based Strategy.

- And, fifth, this combination of a highly tailored NCW–EBS approach appears to offer Australia a true strategic edge—possibly for a generation. In consequence, the real challenge is for the country’s defence and wider national security systems and structures to accept the need for change and to move pro-actively into a process of experimentation and implementation.

\*\*\*\*\*

## ***DISCUSSION***

*Air Marshal Ray Funnell (RAAF Ret’d):* Thanks Ross, I greatly enjoyed that. I wanted to pursue with you the issue of the application of these network centric capabilities at the strategic level. It seems to me that already at the tactical and operational level a lot of it is being done, and being done very well, but I’m concerned about the strategic level. I think we have in the recent past seen where, as a result of inappropriate decision-making at the strategic level, you end up in the wrong place, at the wrong time, doing the wrong thing, and doing it brilliantly. With strategic level decision-making, the important thing is to get those who are involved in that process to think in terms of the wise application of military power. In a paper I wrote back in 1999 on the use of military power in Kosovo, I made the statement in there that modern politicians—not only modern politicians, but politicians in general—do not understand military power and as a consequence they seldom apply it wisely. You mentioned the case of Margaret Thatcher and that came out full well in the Falkland Islands conflict, but certainly she was *sui generis*. I mean, it had not been done before and I’ve not seen that either John Major or Tony Blair did it subsequently, and never to my knowledge in this country, even in major exercises, has the Prime Minister played the ‘Prime Minister’ or any of the senior involved Ministers played their parts as well. Consequently, when it comes to military conflict, they are unused to having to deal with the subjects that come to their table. Now, how do we get these people who will be involved in very major decisions putting our national future on the line? How can we get them involved in developing their own skills in the application of military power through network centric arrangements and to ensure that we don’t make blunders at the strategic level, no matter how well we perform operationally and tactically?

*Professor Babbage:* Thank you Ray. I actually think that you’ve put your finger on one of the most serious challenges we face. A couple of people have already said today that the most serious challenges we face in this whole agenda are actually the human ones, rather than the technical, and I think that’s broadly right. I’d go further and agree with you that I think that some of the most serious ones are actually not the people in uniform or even the people in the Defence organisation, although I think there are some issues there more generally. The most serious problems are in the higher command and particularly at the political level. What can we do about it? There are no simple answers, but I think we’ve got to work a lot harder to make sure that we have better educated and trained staffers that go into key positions. I’m struck by how in the United States, in particular, the Pentagon makes sure that the senior politicians, and not only the Secretary of Defense but people up on the hill, have very

free access and routine access to remarkably senior military advisers all the time, just about as often as they want. And guess what? They're better informed and they know who to ask, and that comes out pretty clearly when you see what happens in some of the key Congressional committees. It means that when politicians move through the system and eventually get to Ministerial level they are, in general I'd argue, better prepared—not perfectly, by a long shot. There are no absolute answers here, but I think we've got to encourage them very directly as well to be involved in more exercising. And I think we have got to give them a 'comfort factor'. I was never involved directly of course in what I understand Margaret Thatcher did in those exercises, but I understand that they were normally pretty small operations. There were normally no more than about 20 people at Norwood in the room on the days when they ran these games and, as a consequence, there was a lot of trust and there was never any leakage. It's clear to me that one of the concerns that senior politicians have on both sides of politics with this sort of activity is the possibility that they may be put on the spot to make a decision in a 'hypothetical', and they make that decision and then it might be leaked. In this country, as you know, there have been a few cases where politicians have played in such things, but they've been far too rare and we've got to find a better mechanism for involving them, training them and giving them a chance to feel their way. In my view, it's going to be more important if we go down the sort of track we're about now, because effects-based operations with NCW—understanding the high level political imperatives there—is going to be far more complex it seems to me than the sort of operations we were looking at 20 years ago.

*Mr Maurice Horsburgh:* Thank you for an excellent presentation. This question is indirectly related to network. I have grave reservations with America's reaction to 9/11. Rather than deal with the cause, the US has treated the symptoms with 'cluster bomb' diplomacy. The Iraqi campaign, by any standards, is an illegal war. We went to war with a plan, which would have made von Clausewitz choke on his sauerkraut or maybe even have a dose of the JTRS, as General Hurd would say. Now I am daily bombarded by pseudo-intellectual, convoluted bulldust by spin doctors, politicians, neocon think-tanks and Fox News. At these conferences, I'm always reminded, 'You must always think out-of-the-box'. But when I think out-of-the-box, this war is all about the profits of Halliburton, Kellogg Brown and Root, and the promotion of Paul Wolfowitz in Cheney's 'New World order' or the project for the new American century. So, a rather provocative question, is Canberra now a wholly owned subsidiary of a cabal of Pentagon neocons, in what is now commonly called 'Israeli-occupied' Washington, and are we totally subservient to the White House? Thank you sir.

*Air Commodore John Harvey (RAAF – Moderator):* I am searching for the NCW connection, but Professor Babbage will make a quick comment.

*Professor Babbage:* Actually, there really is an important point that you're alluding to, I think, and that is the response to 9/11; the response to international terrorism and what I call macro-terrorism, because I think there really are some new elements in the form of terrorism we are seeing now in terms of the apocalyptic ideologies and the not regional, but the global perspectives and global reach and the global intent of some of these groups. And the question that arises in my mind, which is really a lot of what I think you're alluding to, is have we got a strategy for winning? I was in Washington last week and I was in London also earlier last week. One of the issues I was raising

was that we are all spending a heap of money, supposedly on counter-terrorism—I think Australia, if you add it up, is spending about a billion dollars a year now across portfolios on this problem—and one of the key questions in my mind is what is our strategy for winning? And if we don't have a very clear strategy, how do we evaluate the alternative options for actually pursuing key objectives towards securing victory here? My personal view is that, in the end, it boils down to what I'd call political warfare. These people have got to be so alienated within their own societies that they either give up or they're offered over by other members of their families and their communities. Some in the room might think that's asking a bit much, but I'd remind you that we've done this before. One of the best case studies is, in fact, in Malaya in the 1950s and the anti-Communist campaign that was run and General Templar's operations. It was essentially political warfare, supported very strongly by police and military forces in a very subtle and clever campaign. We need to do something like that, but we haven't really got our heads around it yet. What I can say is that this issue was raised with US Secretary of Defense, Donald Rumsfeld, directly at the Shangri-La Conference of Defence Ministers in June, in a public forum, so I can allude to it. Without wanting to go into the fine detail, he spoke for about ten minutes on this issue and how we haven't yet got our head around it properly. So there are plenty of people who are concerned about it. I think we've got to work harder on getting a good answer and soon.

*Mr David Carr (Defence Science and Technology Organisation):* Ross, you mentioned the level of coercion required to get an enemy to act in a certain way. People overseas are doing a fair bit of research in this area, quite clearly. What type of research would you like to see Australia do to enhance our understanding of coercion?

*Professor Babbage:* That's a very good question, and I think there's a lot that needs to be thought about and looked at. In my view, the sorts of operations that might make sense are going to be very culture and society dependent. It depends precisely on who you're wanting to persuade, how much time you're likely to have, what is important to those people and what's not, what their strengths and weaknesses are and all that sort of thing. Clearly, in nearly every circumstance you're going to want a series of layered options to be able to use for coercion. Some of these might start in a very gentle way; just suggesting to someone that instead of doing 'A', they might contemplate doing 'B', and actually situating the environment around them to encourage them to go to 'B'. You would then move up to various forms of more active coercion—stronger suggestions, even semi-threats, moving right through in the end to coercive use of military force, indirect at first and then maybe direct eventually. There are some very interesting twists and things that need to be thought about with this, not least about what it might mean for the level of precision and the level of use and the sort of target sets that might make sense for defence forces to have up their sleeves in these situations. There's a lot of work that needs to be done I think. I also think that we've got to be very careful and one of my biggest concerns, if we move down this track, is to make sure that we're not ethnocentric. That is, we do not jump to conclusions about how we would feel if we were President X, rather than what President X himself and his own society and culture might think. I worry that we don't know enough about, for instance, the Iraqi society or the Iranian society or any country you want to name to understand really what motivates people, how they relate with each other and the sort of suggestions, maybe even pressures, we might want to put on them from time to time to achieve the optimal effect.



# SEVEN PROPOSITIONS ABOUT CLOSE AIR ATTACK ON THE FUTURE BATTLEFIELD

DR ALAN VICK

## INTRODUCTION

This short paper presents seven propositions about close air attack on future battlefields.<sup>1</sup> It is intended to be speculative and somewhat provocative, but at the same time grounded in lessons learned from recent combat operations and ongoing advances in technology.

It is clear from recent combat operations that the relationship between air and ground power is changing. First, Operations *Desert Storm*, *Enduring Freedom* and *Iraqi Freedom* demonstrated that air power is increasingly lethal against ground forces in the open, especially those that are motorised and operate in large formations. Iraqi forces learned to their sorrow in 1991 that night provided no cover for motorised forces on the move. They again learned in March 2003 that severe weather, even a massive sandstorm, would not prevent US and allied intelligence, surveillance and reconnaissance assets from detecting them—whether moving or hiding—and that US satellite guided munitions could accurately attack them with devastating results in the middle of this sandstorm. Similarly, Taliban forces suffered devastating attacks whether in field fortifications or on the move.

Second, recent experience suggests that close air attack should not be viewed as primarily an emergency mission. It is true that in many cases, air can be most effective against enemy ground forces by striking them long before they reach friendly forces. Yet, in situations where the enemy may be dismounted and/or operating in complex terrain, it may be impossible to detect and attack them prior to contact with friendly ground forces. In such situations, rapid, accurate close air attack provides vital fire support. This proved to be the case during much of Operation *Iraqi Freedom* when Iraqi regular forces or irregulars would ambush US and allied forces from built-up areas. Air power quickly became the weapon of choice for those situations due to its precision, lethality and ability to avoid collateral damage.

Third, US ground forces are seeking to become more strategically responsive and more agile on the battlefield. In order to do that, they are reducing artillery fire support for manoeuvre units and reducing artillery unit basic loads of ammunition.<sup>2</sup>

---

<sup>1</sup> I am indebted to my RAND colleagues Bruce Pirnie, Karl Mueller, Adam Grissom and David Orletsky for sharing their work and insights on this topic. These propositions are reflections based upon work that the five of us did collaboratively over the last two years. That work is documented in Bruce Pirnie, et al, *Beyond Close Air Support: Forging a New Air-Ground Partnership*, RAND, Santa Monica, California, forthcoming early 2005.

<sup>2</sup> Adam Grissom at the RAND Corporation has calculated that the shift to new brigade formations (expected to operate in many cases without division and corps fire support) could reduce the weight of fires available to a typical brigade in a notional four to six hour engagement from 600 tonnes to below 100 tonnes. See Bruce Pirnie, et al, *Beyond Close Air Support: Forging a New Air-Ground Partnership*.

New Army concepts are shifting the emphasis from weight of supporting fires to expanded situation awareness, networking and precision fires. These new concepts are creating opportunities for force application from the air to substitute for ground fires.

### **PROPOSITION ONE: AIR ATTACK AND GROUND MANOEUVRE WILL BE PLANNED TO BE MUTUALLY ENABLING**

As we look to a future in which ground forces are becoming more dependent on force application from the air, we need to revisit the nature of the air-ground relationship. Historically, ground forces were the primary killers of enemy ground forces. As a result, the ground commander expected to be the supported commander with other arms in a supporting role. Although there may still be times when one Service component is supported by others, more often air and ground forces will operate as partners. To fully realise the benefits of this partnership will, however, require the components to think differently about their roles. Rather than focusing on supported versus supporting, high performing ground and air forces will plan together and act in order to enable the other component to be more effective. Air attack and ground manoeuvre would be planned in a highly integrated manner, rather than looking at air as part of the fire support plan for a manoeuvre scheme developed independently. In such a highly integrated scheme, air attacks might prepare the battlefield for ground manoeuvre and support offensive ground operations whose primary purpose is to flush enemy forces so air can in turn kill them. Under this concept, supported and supporting distinctions quickly lose meaning. Such operations are more accurately thought of as mutually enabling. Under this concept each component makes unique contributions.

Air attack denies the enemy the ability to conduct offensive motorised operations at the brigade level or higher. During Operation *Iraqi Freedom*, for example, Iraqi forces were able to move brigade-size forces to defensive positions, but air power prevented them from conducting offensive actions at the operational level of warfare.<sup>3</sup> Air power's ability to see throughout the depth of the battlefield and attack motorised formations protected friendly flanks and allowed relatively small units like the 3rd of the 7th Cavalry to operate well in advance of supporting units without undue risk of being cut off, surrounded and destroyed in detail by superior enemy forces.

Ground forces will find dispersed enemy elements, pin them down or force them into killing zones. On future battlefields, opponents will often use complex terrain to hide and in many cases, it will take ground forces to find and identify them. This is especially true for operations against light infantry opponents, insurgents and other irregular forces.

At the tactical level, air will provide fire support for engaged friendly forces. At the same time, air will take the lead in finding and attacking enemy forces that are out of sight of friendly ground forces. This is essential on a dynamic battlefield in which enemy forces may be manoeuvring to attack behind the cover of a ridgeline or other

---

<sup>3</sup> It is true that the Iraqis conducted a brigade-size offensive action at Objective Peach without detection by allied ISR. The brigade was a reserve element from an Iraqi division occupying defensive positions a few tens of kilometres from US forces at Peach. It had a relatively short distance to move and did not constitute manoeuvre at the operational level of warfare. Although there was some fierce fighting, at no point were battalion or larger allied formations at risk.

terrain feature. Air power did exactly this during Operation *Anaconda* where strike aircraft spotted and attacked Al Qaeda reinforcements outside the sight of US ground forces or Terminal Attack Controllers (TACs).

## **PROPOSITION TWO: THE DIGITAL BATTLEFIELD WILL ALLOW MORE AGILE INTEGRATION OF AIR AND GROUND OPERATIONS**

In the past, linear control measures were used to ensure that friendly forces did not accidentally engage one another, to control the speed of advance and to ensure that enemy forces could not exploit seams between friendly ground forces. With respect to air and ground operations, the Fire Support Coordination Line (FSCL) became the key measure. The FSCL was established by the corps commander and situated along a prominent terrain feature, such as a river. It would typically be placed 100 to 150 kilometres ahead of the forward line of friendly forces. Beyond the FSCL, air operations did not require the approval of the ground commander. Short of the FSCL, all air strikes required approval by the ground commander, although this was typically delegated to USAF or USMC terminal attack controllers working with ground manoeuvre units.

This approach worked reasonably well for linear operations, although several problems were encountered. First, it is difficult to know how far out to place the FSCL. If the FSCL is placed too far out, it creates a huge area beyond the range of ground force weapons in which enemy forces might find sanctuary. Enemy forces located many tens of kilometres from friendly ground forces would typically not be visible to terminal attack controllers located with friendly ground forces. Although arrangements existed that allowed air forces to attack these enemy elements, often command and control problems prevented effective attack. If the FSCL were placed too close and friendly forces advanced rapidly, they could overrun the FSCL. In this case, the advance would be halted because of the risk of attack by friendly aircraft in the forward zone. The FSCL also only works on a linear battlefield. It is not an effective way to control fires on dynamic, non-linear battlefields.

In the future, digital geopositioning and networking technologies should allow the FSCL to be replaced by a 'kill box' fire support coordination system. Kill boxes have been used in recent operations to supplement the FSCL. A theatre of operations is divided up into kill boxes, 30 minutes latitude by 30 minutes longitude in size (roughly 30 nm by 25 nm for kill boxes in Iraq). Air and ground staffs working together determine which kill boxes are open for air fires and which are closed. The limit in this system today is the lack of a digital system to update kill box graphics across the theatre in near real-time. Voice communication was used to open and close kill boxes in Operation *Iraqi Freedom*, significantly limiting their utility. On future battlefields, digital networking should allow this to be done rapidly, with updates flowing to cockpits and ground forces on a regular basis.

## **PROPOSITION THREE: CLOSE AIR ATTACK WILL GROW IN IMPORTANCE ON FUTURE BATTLEFIELDS**

As noted above, the relative importance of close air attack is likely to grow on future battlefields. There are several reasons for this. First, combatants facing US or other

advanced air power are likely to learn from recent conflicts and not present massed targets that are easy to detect and attack from the air. Rather, they will disperse, hide in complex terrain and take other steps to avoid being detected. If this is right, air power will have fewer opportunities to attack enemy forces far removed from friendlies. Rather, friendly ground forces will often discover the enemy through contact. As a result, air-ground mutual dependence will grow. Air will be more dependent on ground forces to find a dispersed, hiding enemy. Similarly, ground forces will operate in smaller elements to find this dispersed enemy and will look to air for fire support when they come into contact.

#### **PROPOSITION FOUR: NETWORKING OF GROUND ELEMENTS, TERMINAL ATTACK CONTROLLERS AND AIRCREWS IS KEY FOR FUTURE JOINT AIR-GROUND OPERATIONS**

Terminal Attack Controllers (TACs), either on the ground or in the air, play an essential role in air-ground operations today. The TAC bridges the gap between the capabilities that air power brings on the scene and the needs of the ground commander. TACs are expert in the tactical application of air power and aircraft control procedures and have a deep understanding of ground force operations. They ensure that air attacks hit the right targets with the right munitions and are key to avoid fratricide.

Operation *Enduring Freedom* in Afghanistan established a new model for the air-ground partnership with US Army Special Forces, USAF Combat Controllers (CCTs) and Enlisted Terminal Attack Controllers (ETACs) working closely with indigenous Afghan forces and allied air power. The USAF CCTs and TACs were able to bring air power to bear in a way that gave the Afghan Northern Alliance the edge against the Taliban, leading to a quick victory and overthrow of the Taliban regime. CCTs and ETACs again proved their worth during Operations *Anaconda* and *Iraqi Freedom*, convincing the US Army that it needs TACs not just at the battalion level (where they currently reside) but also for every manoeuvre company and Special Forces A-Team. As a result the demand for TACs could double over the next decade. Unfortunately, TACs cannot be created quickly or cheaply. The job is highly demanding and relatively few people can do it. Additionally, it takes several years of training and experience before a TAC can be fully certified to control strikes and close to 20 controls a year to remain proficient. Thus it seems unlikely that TACs can be provided for every US Army company and A-Team anytime soon.

As we look to the future, networking of the engaged combat element, TAC at the battalion command post and aircrew is likely to make it possible to provide rapid and accurate air strikes for dispersed ground forces without necessarily providing a TAC with every unit. The key to doing this is disaggregating the TAC function. TAC responsibilities currently include the following:

- **Deconflict aircraft in target area.**
- **Assign aircraft to targets.**
- **Select munitions.**
- **Assign attack headings.**
- **Clear hot.**
- Deconflict land forces.

- Validate targets.
- Identify targets.
- Adjust aimpoints.
- Assess battle damage.
- Call for close air support (CAS).

Of these, only the responsibilities in bold require a fully certified TAC. The others already are shared with others or delegated. Evolving technologies are likely to provide opportunities for others to take on some of these tasks, allowing the TAC to function on those functions that require an airman.

On a networked battlefield, the engaged ground force, the TAC working out of the battalion Command Post (CP) and the aircrew on the strike aircraft will work together in a more agile fashion than is possible today. The engaged ground force element should have the means to identify precisely their own position and, using devices that combine a laser rangefinder, GPS receiver and compass, determine the coordinates of enemy forces. The Viper and Mark VII systems are two such devices used successfully in combat in both Afghanistan and Iraq. These systems, however, are not user friendly, requiring a high degree of training and experience to use correctly. The user also must do trigonometric calculations to get accurate coordinates; something that many would find challenging at a desk, let alone under fire.

In the future, such systems are likely to be much easier to use. Future platoon leaders will have at their disposal handheld digital devices that do those calculations as well as send digital calls for fire to the battalion CP. The TAC working with the fire support officer at the battalion CP would then confirm the target is valid, add additional information to the call for fire and then send it digitally to strike aircraft. The TAC, using voice or a digital data link, would clear the aircraft to hit the target.

Finally, strike aircraft would come on the scene with considerably more information than they have today. Blue Force tracking systems will provide the location of friendly forces within whatever radius the aircrew finds helpful. Depending on system latency in the Blue Force network, this information may be several, perhaps many, minutes old. If that is the case, strike aircraft will need access to near real-time information also. There are a couple of ways they might get that. First, aircraft could be fitted to receive transmissions directly from the friendly forces within line of sight. US F-16 aircraft equipped with the SADL system were able to do this during Operation *Iraqi Freedom*. Alternatively, ground forces might use tagging devices that could be picked up by aircraft radar. Finally, strike aircraft will have improved sensor pods and air launched mini-UAVs to provide high resolution imagery of the target area. The combination of these technologies and concepts should increase the availability of air power to dispersed ground forces, reduce the need to have TACs with every manoeuvre element and reduce the risk of aircraft striking non-combatants or friendly forces.

#### **PROPOSITION FIVE: BOMBERS WILL EVOLVE INTO GUNSHIPS, PROVIDING ON-CALL FIRES ACROSS THE BATTLEFIELD**

The bomber's long range, long endurance and large payload made it ideal for operations in Afghanistan and extremely useful for operations in Iraq. Initial air

operations over Afghanistan had to be conducted from remote land bases or from carriers in the Indian Ocean. As a result, naval aviation and bombers flew most of the strike missions. B-52 and B-1 bombers struck Al Qaeda and Taliban forces throughout the country. In numerous battles, bombers provided fire support that enabled Northern Alliance or other friendly land forces to rout enemy forces and capture key terrain. In some cases, bombers saved small friendly forces from being overrun by much larger Taliban forces.

In the future, friendly forces may need on-call air power available over prolonged periods. Long range, long endurance aircraft are well suited to such missions, particularly if they have enhanced capabilities to work directly with friendly ground forces. One idea would be to modify some B-52 bombers to give them a capability that combines the best features of a heavy bomber and the AC-130 gunship. A B-52 bomber modified for the gunship role would have the following characteristics:

- Digital links to TACs, ground forces, sensor platforms, and other strike aircraft.
- Advanced targeting pod.
- Air-droppable mini-UAVs.
- Air-droppable unattended ground sensors.
- Six-man crew.
- Menu of weapons.

Digital links would allow the gunship, ground forces, nearby TACs, Airborne Forward Air Controllers and ISR/C3 aircraft to share imagery, intelligence, target location data and Link-16 type data on the fuel state and weapons load (among other things) of other strike aircraft. An advanced targeting pod would provide high resolution imagery for the gunship operating at medium altitudes in addition to a variety of other targeting tasks. Air-droppable UAVs and ground sensors would provide the gunship with an autonomous ability to get high quality imagery or other sensor inputs from a priority area. A six-man crew would include the pilot/aircraft commander, copilot, offensive weapons officer, electronic warfare officer, terminal attack controller and off-board sensor operator. The off-board sensor operator would use the vacant position formerly occupied by a gunner. He would launch, control, and monitor mini-UAVs and unattended ground sensors, which would allow the B-52 to see targets below a cloud ceiling or too small to see clearly from higher altitudes. New crew coordination procedures would likely need to be developed because neither AC-130 practices for a 13-man crew nor traditional bomber procedures are a perfect fit.

A weapons suite takes advantage of the ability of B-52 to carry a large mix of munitions. For example, it might carry JDAMs on its outboard pylons and a variety of other precision weapons carried internally.

## **PROPOSITION SIX: GROUND AND NAVAL INDIRECT FIRES WILL REMAIN AN IMPORTANT SOURCE OF FIRE SUPPORT FOR GROUND FORCES**

Heavy bombers, current era gunships and fighters can all provide on-call fire support for engaged ground forces. This is fairly straightforward to do during an intense combat phase, such as the drive up the Euphrates River Valley during Operation *Iraqi*

*Freedom.* Modern air forces can generate many sorties, providing around the clock support if the operation is bounded by space and time. If, however, operations are spread out over a large area, combat occurs sporadically and the mission lasts months or years, the force structure and manpower cost can be huge. For example, an Iraq size country would require a force of well over 1000 fighters to provide 12-minute response times 24/7 indefinitely.<sup>4</sup>

For these reasons, mortars and artillery are likely to remain the least costly way to provide immediate fire support across a theatre of operations. This is especially true for counter-battery fire where response times generally have to be under five minutes. Naval gunfire can provide this support as well for littoral scenarios. Attack helicopters might also provide this support, although their relatively slow speed limits the size of area they can cover from ground alert positions. On-call air power is best suited to support planned offensive operations, high priority regions, missions or units. Aircraft can also act as a theatre reserve, able to generate considerable combat power within a short period of time. Strip alert aircraft throughout a theatre can quickly reinforce at a much lower cost in aircraft and crew than airborne alert.

### **PROPOSITION SEVEN: ENEMY AIR DEFENCES WILL HAVE A MIXED IMPACT ON CLOSE AIR ATTACK**

Recent air operations in Afghanistan and Iraq have faced relatively limited air defences, particularly at medium altitudes. As a result, ISR platforms, non-stealthy bombers, tankers and other aircraft could loiter for hours over the battlefield. This allowed concepts of operation that would be prohibited in the face of more advanced air defences.

At the same time, trash air defences (eg. small arms, RPGs, medium and heavy machine guns, 23 mm and other AAA) and MANPADS remain a threat at lower altitudes. This is especially problematic for attack, scout and air assault helicopter operations, airlifters, and AC-130 gunships.

This suggests that close air attack using concepts, platforms and munitions from medium altitudes will be largely unconstrained in most contingencies. In contrast, the deployment of advanced air defences would raise questions about the viability of current close air attack concepts.

In the face of advanced radar guided SAMs, airborne FACs would probably not be survivable and non-stealthy aircraft would have to operate in a much more guarded way. Close air attack under these conditions would likely emphasise a major SEAD effort to start. Ground forces would play a large role in detecting and destroying advanced battlefield air defences. In the initial period of combat, stealthy bombers and fighters, UCAVs and UAVs would be required for close air attack. To the extent that advanced air defences constrained the effectiveness of close air attack, ground or naval-based fire support would rise in importance.

---

<sup>4</sup> Thanks to RAND colleague David Orletsky for sharing his calculations on on-call fires. See Pirnie, et al, *Beyond Close Air Support: Forging a New Air-Ground Partnership*, for more details.

## CONCLUSIONS

My hope is that these seven propositions will contribute to a constructive debate about the future of air-ground operations. Ground and air forces are still internalising the lessons from operations in Afghanistan and Iraq. Soldiers and airmen appear to be agreed on some key lessons (eg. the growing importance of CAS), but on others (eg. the utility of linear fire support control measures) they remain far apart. No one Service, if left to its own devices, is likely to get this entirely right. Rather, a multi-Service dialogue is needed to embrace fully the potential of new technologies and develop concepts that most effectively combine the unique capabilities of ground and air forces.

\*\*\*\*\*

## DISCUSSION

*Air Commodore John Harvey (RAAF):* One of the concepts you mentioned in your talk was the concept of supported versus supporting forces becoming less meaningful in the future. One thing I've been thinking about is the sensor versus shooter. As I see it, that's becoming fairly interchangeable nowadays as well. Would you like to comment on that approach? In some cases the aircraft is the sensor for the shooter on the ground and other times it changes and can flip-flop between them.

*Dr Vick:* I think this is what we've heard all day today; the requirement for agility on the future battlefield and that there is a dynamic nature to future operations, either because that is the way we want to operate or the way we think we have to operate to defeat certain kinds of foes. In that dynamism you have the sensor and shooter perhaps flip-flopping; the supported versus the supporting going back and forth. This is why in our work we emphasise this concept of mutually enabling operations of a partnership—you can argue that joint forces have been partners for many decades—but a level of partnership and a level of integration that we've found difficult to accomplish in the past.

*Mr Phillip Rechter (Agent Oriented Software):* Alan, with regard to UCAVs and UAVs, which you just had up there on the last slide, we see in Iraq the firing of missiles etc, obviously with the man in the loop. I think it will still be a long time before we see truly autonomous UCAVs and UAVS with firing capabilities. Would you agree with that and how far out do you think that would be?

*Dr Vick:* I think that is a good point. In some earlier work that we did at RAND on elusive targets we looked at the LOCAAS system [Low-Cost Autonomous Attack System], which I am sure a number of you are familiar with, that was designed to be an autonomous weapon; it was like a cruise missile and had, maybe, a 100-mile range. It would go out and use a laser radar [ladar] and an advanced automatic target recognition system to identify enemy armoured vehicles and attack them. We looked at that for operations, such as *Allied Force* in Kosovo, and said there was no way that your commanders or national leaders would be comfortable with that kind of system

without a man in the loop, because it might go out and accidentally decide that a school bus full of kids was a target and take it out. So I think those sort of weapons are going to be limited to situations where you're convinced that within this area of say 50 by 50 kilometres, or whatever, it's just empty in there and there are only enemy forces, and that's going to be a rarity most of the time.

*Lieutenant Colonel Jim Bryant (Army):* My thanks for your presentation. Like you, I'm a light infantryman, but perhaps not so light any more. I guess it is an old chestnut but I have a question about assured fire support. The problem from a 'ground pounder's' aspect is that he doesn't trust that indirect fire support unless it is virtually organic. That's obviously unrealistic, especially in the new scenarios of kill boxes etc. How do you envisage the command relationship between the Battalion Commander and his supporting air assets, either Army or Air Force, in this new environment and how flexible will that have to be? How can we assure support where it's required when there may be competing tasks? There's often an argument between infantry and artillery internally about assured fires? Is the priority of fire counter-battery, or is it support to the manoeuvre commander? I was wondering about your thoughts on that aspect sir?

*Dr Vick:* A very good question and I think that's an essential point. I would think any sensible ground commander is going to always want to have as many fires organic as he can and you probably never want to get rid of your mortars for that reason. But as we look to these mutually planned operations in which you say, 'Well we've got a priority operation here and, as part of that planning, the coalition forces are going to put these orbits over this force that, say, is on the vanguard and you're going to have this many two-ships overhead 24-7', and they're coming from our allied partners, they're coming from the Marines, Navy, Air Force and perhaps Army attack helicopters are woven into that, but I agree with you that you have to have some guarantee that they will be available. Now, there might be weather or some factor that limits them in a particular situation, but you have to know when you go in there that you have a certain amount of fire support available or you can't really plan your operation; so you have to have that. In talking with artillerymen—it's funny they often sound like airmen when they talk about manoeuvre commanders—they'll complain and say, 'The manoeuvre commander works out his ground manoeuvre scheme and then only later will he start thinking about fire support'; although that is certainly not true for all manoeuvre commanders. What we're suggesting is planning at the same time, in which the air and ground components are working very closely and mutually developing this plan, as opposed to the ground commander levying a requirement on the air component.

*General Hurd:* If I could just make an additional comment on that. I've got kind of a different view of the future as we continue to get more precision type weapons and more ISR to support the battlespace. Your question's a very valid question and, at the end of the day, I don't think the Army is going to walk away from all organic fire; you'll always maintain that. But I have a view that CAS [close air support], as we have known it for most of our lifetime, will really be an emergency CAS because with the ISR that we've got today and what we are building for the future there should be no way that a large enemy force, mainly 'mech' [mechanised] or armour, should ever be able to slip up on a coalition force. I mean, if it happens, we're 'asleep at the wheel'; it's our own fault. I see that air power's role is to put that ISR out there and to

be able to find that force and then cut that force down to the size that we can lever it into the land forces at an amount or a rate that he can afford to take that force on with his organic fires and his organic capability. I think that ISR is the key to that in the future and I think we're building that. If you compare *Desert Shield/Desert Storm* to what we've got today, we're probably fourfold already and God only knows how many UAVS we'll have in another two years. I view that a little differently than maybe what we're talking about today as we project into the future. I think Alan [Dr Vick] is right, maybe today, but I think that's rapidly going to change in the next two or three years. Alan, would you comment on that?

*Dr Vick:* General Hurd, I agree with you but I think, for the reasons that you outlined, our adversaries are not going to present those massed forces. You're absolutely right, if they are foolish enough to do that, with the systems you describe we will find them and kill them. That is why, in my view, we will see less and less of that. We are already seeing this today with insurgents and other asymmetric strategies but we are going to see adversaries seeking alternative ways of achieving their objectives and the challenge for airmen and for soldiers will be to deal with forces operating in heavy foliage and difficult terrain in urban areas, in small dispersed elements, in many cases without vehicles. So, I'm completely in synch with you but I don't think we've got the sensors and the ISR systems yet that can tell us, 'Oh yes, there are a bunch of guerrillas moving through the foliage'. Technically we can, but we've not made the effort yet. There are things that we could do—foliage penetrating radar, hyperspectral image processing—but we've not really made the investment yet.

*Group Captain Chris Finn (RAF – Director Defence Studies (RAF)):* I am minded, if I may very briefly, to quote Marshal of the Royal Air Force Tedder after the attack on Caen who said, 'We must cure the Army of this addiction to the strategic bomber', and that I think has come out in some of the themes here. But to go on again from the previous questioner, when you go back to the Cold War era we used to train all the time in RAF Germany with 1 (BR) Corps; we would do close air support all the time and the Army would always see the Air Force. Now we are moving to precision guided weapons delivered from 15 to 25,000 feet, we cannot see that any more and we can't really drop a 14 kilogram practice bomb in that sort of environment to give the point that we're still around. How are you actually looking in your studies at how we can address this problem of training and confidence?

*Dr Vick:* Chris, that's a great question. I know it's something that US airmen, such as Colonel Matthew Neuenswander who used to command the Air Ground Operations School at Nellis [Air Force Base] and others, are very much worried about. We have a number of problems in the United States. One is, we have very few places in the country where we can actually do ground manoeuvre and air-ground operations in the same place. There are plenty of places where you can fly aircraft and there are places where you can move ground forces, but you can't do both. So that's a problem there. It's also the case that for the Army they have a long list of training requirements when they send a Brigade out to the NTC, or National Training Center, and working with airmen and integrating CAS has not been the highest on that list. We've got a lot of combat vets now but before that you had people going through NTC and not really getting a real world experience of just how artillery and air power would be integrated. I think that's something we've not quite figured out how to deal with but it's an increasingly high priority.

*Air Commodore John Harvey (RAAF):* I have a question relating to one of the issues flowing from that operational analysis work, the number of aircraft to cover the area, I note now we can see and communicate at the speed of light, but we can only attack at the speed of the weapon. Is there much work going on at RAND looking at increasing the speed of weapons or other weapons that can solve the problem in a different way?

*Dr Vick:* One of the things we looked at a few years ago was hypersonic weapons and they certainly are of interest for some missions if you're going after enemy mobile air defences or mobile ballistic missiles. For this close support mission, I'm not sure. Even hypersonic weapons can't be on the other side of the continent if you need a five minute response time. They'd have to be within a few hundred miles and then you've got some terminal guidance issues of how do I get that weapon slowed down and a precision effect out of it, but they're certainly worth pursuing.

*Air Commodore John Harvey (RAAF):* In the longer term, are there future energy, non-mechanical type weapons? Are they possible as well?

*Dr Vick:* Sure, but I don't have any particular inside information on that.

*Group Captain Dave Richardson (RAAF):* Sir, with the US Army's decision to cancel Comanche and, I understand, studies with the USAF to extend the A-10 life out to 2028 and your awesome depiction of a B-52 gunship, is there any link between your seven propositions and what appears to be a rebalancing of the fixed and rotary winged assets expected to be used on the battlefield? Forgive me for asking a simple hardware question.

*Dr Vick:* No, it's a very interesting question. I've not been briefed on the latest Army thinking. I know that US Army aviators took a deep breath after the experience of the 11th [Attack Helicopter Regiment] at the Karbala Gap and the losses they had with the Apaches, and are rethinking some of their tactics, techniques and procedures. I've not seen any draft new doctrine from the Army. Certainly, the Israelis are reported to have decided that the armed UAV is a better way to go for many missions than the attack helicopter. I'm not sure that that is a conclusion that the US Army would draw but, at the least, they're rethinking the way to use the attack helicopter. For example, in the past attack helicopters advanced on line at low altitudes (300 feet) and slow speeds (20 knots) that made them extremely vulnerable to ground fire. Now they are looking at running fire at more reasonable speeds, jinking and doing things like that. I believe they're looking at a small scout helicopter to replace the Comanche, something for example like the Little Bird that's much more agile and harder to shoot down. In terms of rebalancing, I'm not aware of any formal [US] Department of Defense effort that looks at rotary wing, and rotary winged assets are viewed as having a different mission. In fact, the US Army doesn't consider the attack helicopter a close support weapon; they consider it a manoeuvre force.



# **SAY AGAIN? – A (VERY) BRIEF HISTORY OF NETWORK CENTRIC WARFARE**

**DR ALAN STEPHENS**

The essence of network centric warfare (NCW) is, as with many things in life, effective communication. By ‘effective communication’ I mean a process through which various numbers of people, ranging from a minimum of two to potentially thousands, exchange information that is useful, timely, and comprehensible. Thousands will be involved when the kind of advanced force structure envisaged by the most optimistic speakers at this conference is realised: a structure that will be characterised by such aphorisms as ‘system of systems’ and ‘global information grid’, in which ‘every soldier is a sensor’. At the other end of the scale, a network exists when two people cooperate to make the whole greater than the sum of the individual parts.

In the case of air combat (the form of military power with which this paper is primarily concerned), networks in their most basic form came into widespread existence early in World War I, when pilots and observers realised that they were likely to be more effective if they worked as a team rather than as two individuals. Initially a code of hand signals was used to communicate; later, when aircraft were fitted with speaking-tubes, a standard operational lexicon emerged as airmen sought to minimise the dangers of misunderstanding. Terms such as ‘Tally Ho’, ‘Splash One’, ‘Bogey Dope’, and ‘Holding Hands’ might sound like the conversation within a group of fighter pilots having a night out on the town, but in fact they were devised to try to achieve clarity and brevity while exchanging information in combat. A basic principle of NCW had emerged.

Just as the benefits derived from two individuals in the one aeroplane networking quickly became apparent, so too did the benefits of networking a number of aeroplanes; that is of concentrating force through formation flying. Once again, effective communications was the essential glue. Because practical air-to-air radio communication was not developed until after World War I, visual signalling (wing-wagging, hand signals, and so on) was used to transform individual weapons systems into networks.

By the way, while on the subject of formation flying, in the course of researching this paper, I was pleased to learn of a hitherto unsuspected enthusiasm for that particular expression of network centric warfare on the part of one of the towering military figures from the 19th and 20th centuries, Lord Horatio Kitchener. The Royal Flying Corps’ (RFC) official historian has recorded that, as Secretary of State for War, Kitchener took a keen interest in the development of military aviation, especially the theory of strategic bombing, a notion that would require aircraft to attack in large formations to achieve the necessary concentration of force. Soon after the outbreak of World War I, Kitchener issued instructions to the commander of the Army’s Military [Aviation] Wing, Colonel H.M. Trenchard:

‘Trenchard, when I come down to Farnborough I want to see machines flying in formation’.

‘But that is impossible’, said Colonel Trenchard. ‘The machines are all of different types and different performances; we cannot fly in formation’.

‘Trenchard, when I come down to Farnborough I want to see machines flying in formation’.

‘But, Sir, it cannot be done’.

‘Trenchard, when I come down to Farnborough, you will have four machines paraded for me, to fly in formation’.<sup>1</sup>

The official historian noted diplomatically that, while Lord Kitchener’s foresight was unerring and his will strong, the facts were too stubborn even for him, and it proved impossible for the RFC to ‘fly our machines in formation’ for about a year.

A variation of air power-enabled NCW emerged when air forces began to provide information to armies and navies in near real-time, with artillery spotting initially constituting the main task. Numerous air-to-ground signalling methods were tried, including visual (Very flares, lamps) and wireless. Wireless transmission (W/T) clearly held the greatest potential but initially the technology was not up to the job as radio sets were too large and heavy for the aircraft of the time.<sup>2</sup> But by early 1915 both the weight and the dimensions had been reduced and one-way communication from air to ground became common.

But reflecting the truism that there is more to warfighting than mere technology, problems of interpretation and comprehension adversely affected this embryo network. Soldiers could not understand airmen, and airmen could not understand soldiers. We should not be surprised that the answers to this early instance of what was to become a long-running saga were eventually found in a combination of better liaison between the two groups, the development of a common operational language, and specialist training. Testimony to the ultimate effectiveness of this early venture into three-dimensional NCW can be found in the fact that 60 per cent of all casualties in World War I were caused by artillery fire.

Incidentally, given the claims of originality made for so-called ‘time sensitive targeting’ during Operation *Iraqi Freedom* in 2003, it is noteworthy that in April 1915 a future Royal Air Force Chief of the Air Staff, Major W.G.H. Salmond, devised a system through which corps artillery batteries could immediately be called into action against high-value ‘fleeting’ targets, such as a battalion or a battery on the move, or a large resupply convoy. The transmission by an RFC crew of the message ‘JJ’ together with the target’s position amounted to an instruction for all guns to immediately engage.<sup>3</sup>

The remit for this rudimentary air/land network was expanded to incorporate friendly manoeuvre for the first time at Neuve Chapelle in March 1915. Using a technique

---

<sup>1</sup> Walter Raleigh, *The War in the Air*, Vol. I, The Clarendon Press, Oxford, 1922, pp. 431–32.

<sup>2</sup> In 1914 a W/T set could take up all of the observer’s cockpit, and weighed around 30 kilograms—dimensions which prevented their use in aircraft. H.A. Jones, *The War in the Air*, Vol. II, The Clarendon Press, Oxford, 1928, pp. 82–4.

<sup>3</sup> Jones, *The War in the Air*, Vol. II, pp. 120–21.

which came to be known as the ‘contact patrol’, an airborne observer was tasked with determining the position of advancing friendly forces, information which previously was not readily available to field commanders, and which could be enormously important for decisions regarding supporting artillery fire, protecting flanks, committing reserves to battle, and so on.<sup>4</sup>

Initially the information gathered by airborne contact patrols was passed to army headquarters either by dropping hand-written messages to reporting centres, or by making a telephone call after landing; but within two months these methods had been superseded by air-to-ground W/T. The procedure appeared straightforward. When friendly land forces reached pre-planned positions, they laid out large white strips on the ground, thereby, it was hoped, clearly identifying who was where. As can often be the case, however, the human factor intervened to render the system largely ineffective; in particular, army units could be difficult to distinguish, especially when they forgot to take or display their white strips, as sometimes happened. Liaison between air and ground forces led to the introduction of formal training and the replacement of cloth strips with more visible smoke flares and lamps, and the results improved markedly. Nevertheless, difficulties in exchanging accurate information between land and air forces persisted throughout the war.<sup>5</sup>

Air was also the necessary link in the early establishment of three-dimensional networks at sea, with the spotting flights conducted for naval gunfire onto land targets during the Dardanelles campaign in April 1915 being described by one of the officers of the battleship HMS *Prince George* as ‘a revelation to most of us’.<sup>6</sup>

The common link in those early networks was the aeroplane or, more accurately, the information that could only be provided by the crew of a machine that introduced a revolutionary degree of perspective and speed to the battlespace.

Integrated air defence systems provide my final example of emergent complex networks from World War I. Audacious daylight air raids by the Germans were the catalyst for the construction of the system developed in 1917 to defend the greater London area. Commanded by Brigadier-General E.B. Ashmore, after whom it became known, the air defence network combined coastal spotters (who both watched and listened for enemy bombers), fighters, anti-aircraft artillery (AAA), searchlights, and barrage balloons. Tying all of the sensors together was a centralised command and control arrangement which made up for its technical deficiencies through the systematic approach and doctrinal rigour it represented.

Because communications and, therefore, integration, within the Ashmore system remained patchy, operational responsibility was devolved more by the demarcation of geographic boundaries than by synchronised near real-time decision-making. This approach, by the way, should be familiar to any military professional who practised

---

<sup>4</sup> H.N. Wrigley, ‘Precis of a Lecture on the Development of Cooperation with the Army During the War of 1914–1918’, in Alan Stephens and Brendan O’Loughlin (eds.), *The Decisive Factor: Air Power Doctrine by Air Vice-Marshal H.N. Wrigley*, Australian Government Publishing Service, Canberra, 1990, pp. 94–5; and Jones, *The War in the Air*, Vol. II, pp. 179–81, 232–33.

<sup>5</sup> Wrigley, ‘Precis of a Lecture on the Development of Cooperation with the Army During the War of 1914–1918’, pp. 94–5.

<sup>6</sup> Jones, *The War in the Air*, Vol. II, p. 29.

so-called joint warfare in the last four decades of the 20th century, when the emphasis lay as much on deconflicting friendly forces as it did on having them fight in the same place at the same time. Thus, among other things, the Ashmore system was based on a series of separate defensive rings, within which barrage balloons, fighters and AAA all had their own space, and which other elements of the network entered at their peril. Still, given the technological limitations of the era, General Ashmore's achievement was impressive.

A mere 20 years later the Royal Air Force (RAF) drew on Ashmore's legacy. Utilising immense improvements in W/T, and adding the Chain Home radar system and an excellent centralised command and control organisation, the RAF constructed a networked defensive barrier that the Luftwaffe ultimately could not overcome.

Technology in the form of two-way radio and aircraft intercommunication was also central to two other conspicuous examples of network centric warfare from World War II that I wish to highlight.

The first, involving the RAF's night bomber offensive against Germany and Italy, was remarkable for the way in which it both exploited and ignored NCW. Once the bomber offensive was fully mobilised it was common for around 500 crews and aircraft to participate in any single raid. Inside every one of those aircraft there was a complex network of about seven men, each with his specialist task, and who constantly exchanged and acted on real-time information. Yet externally, the 500 crews could fly for seven or so hours in close proximity and never exchange a word. At one and the same time the bomber offensive represented the exemplar of networked concentration of force and the antithesis of networked information.<sup>7</sup>

External communication was crucial to my second example, the most potent air/land networking of the 1930s and 1940s, Nazi General Heinz Guderian's blitzkrieg. 'Lightning war' consciously exploited the new-found speed and concentration that air and mobile armour had brought to the battlefield, and for the first year of World War II proved near-irresistible.<sup>8</sup> Among other things, blitzkrieg relied on the closest possible coordination between air and land forces engaged with the enemy, a situation fraught with danger should that coordination break-down. It is perhaps no coincidence that Guderian's first professional skill as a junior officer in the German Army before World War I was as a communications specialist.

We sometimes forget that the fundamentals of blitzkrieg were quickly learnt by the Allies, who eventually were more successful than their enemies in mastering the complex challenges of tying air and land forces together. Indeed, it is arguable that the greatest exponent of air/land warfare during World War II was an Allied commander, the Australian-born, New Zealand raised, RAF officer, Air Marshal Sir Arthur

---

<sup>7</sup> It was the case that a designated 'master bomber' or 'pathfinder' might provide target tracking and marking guidance for the main force, and that this could be regarded as a form of information networking. But the fact remains that individual elements of the main force rarely exchanged messages.

<sup>8</sup> It is simplistic to credit any one individual as the architect of blitzkrieg, but Guderian is widely regarded as a major contributor to, and highly successful practitioner of, the concept.

Coningham.<sup>9</sup> Demonstrating admirable clarity of analysis, Coningham refined his task of turning the Desert Air Force into a war-winning tool into three major components: the first, technical/logistic; the second, organisational; and the third, inter-personal.

It would be seriously misleading to understate the difficulties inherent in assembling the right kinds of hardware to fight a war, and in constructing an organisation that enables the chosen courses of action. At the same time, ultimately, we have to fight with what we have got; and also we might reasonably expect that most military professionals would be capable of assembling an organisation that at the least did not hinder progress. By contrast, history suggests that we might be far less confident about the third component of Coningham's trilogy, namely, inter-personal relations. Here, given the often acrimonious relations between the soldiers and airmen of that period (and indeed of subsequent periods), Coningham's response to this perennial challenge was elegantly simple. Rejecting past practice, he insisted that, whatever else might or might not happen, his and his staff's headquarters and living quarters were to be collocated with those of their army counterparts. Coningham knew above all else that if he could not communicate effectively, he could not network. And his definition of 'communicate effectively' did not simply encompass the technological means, but rather the full human dimension of the single most important skill that each of us needs if we are to succeed in any organisation.

Noting the aphorism that we learn more from our failures than from our successes, what a contrast the personal and inter-Service cooperation that characterised the Allies' North African campaign in World War II provides with aspects of the American-led war in Indochina from 1962 to 1972. Specifically, during Operation *Rolling Thunder*, United States commanders divided North Vietnam into seven geographic 'route packages', with the USAF being responsible for striking targets in two of the 'packages', the USN in four, and the commander of American forces in South Vietnam, General William C. Westmoreland, in one. In what was the antithesis of networked planning and operations, there was almost no liaison between the three tasking authorities. Rejecting frequent representations, the Navy refused to integrate all strikes through one headquarters; consequently, according to one of the campaign's most senior commanders, *Rolling Thunder* degenerated into a 'competition' between the Air Force and the Navy to fly the most missions, regardless of conditions and/or strategic objectives.<sup>10</sup>

Remnants of that corrosive kind of rivalry seem to have been evident 20 years later during Operation *Desert Storm*, when incompatible communications systems prevented air campaign planners in Riyadh from transmitting daily air tasking orders electronically to the USN, instead having to print the (enormous) document and have it flown out to the fleet via courier aircraft.<sup>11</sup>

---

<sup>9</sup> For the best assessment of Coningham, see Vincent Orange, *Coningham: A Biography of Air Marshal Sir Arthur Coningham, KCB, KBE, DSO, MC, DFC, AFC*, Methuen, London, 1990.

<sup>10</sup> Wayne Thompson, *To Hanoi and Back: The US Air Force and North Vietnam, 1966–1973*, Smithsonian Institution Press, Washington, 2000, pp. 18–19; Mark Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*, The Free Press, New York, 1989, pp. 129–30. The officer cited was Lieutenant General Joseph H. Moore, Commander of the 2nd Air Division.

<sup>11</sup> Richard P. Hallion, *Storm Over Iraq: Air Power and the Gulf War*, Smithsonian Institution Press, Washington, 1992, p. 256.

One of the more publicised images from recent years shows a US Special Forces soldier on horseback, dressed like an Afghani tribesman, equipped with a notebook computer with which he can call in near-instantaneous precision air strikes from orbiting bombers. Many observers believe that that image from Operation *Enduring Freedom* in 2001–2002 defined the arrival of network centric warfare onto the mainstream military agenda. While the particular operation falls far short of the mature NCW construct envisaged today, the degree of flexibility, spontaneity and individual decision-making it implies clearly differentiates it from preceding forms of air/land operations.

Exactly where the impetus for this new model originated is unclear, but at a conference sponsored by the Royal Australian Air Force it seems only proper to recall the publication ten years ago by the Air Power Studies Centre of a paper titled ‘Employing Smart Technology in Low Intensity Conflict’.<sup>12</sup> Written by the then Officer Commanding No 82 Wing, Group Captain Peter Criss, that paper examined ways in which advanced air power could be employed innovatively in conflict short of theatre or major campaign levels. Specifically, Criss identified a concept of operations in which an F-111 fitted with a target designation system and armed with precision guided munitions could network with small, highly mobile groups of Special Forces, to dominate a variety of contingencies. The paper attracted a good deal of favourable international comment at the time.

If the picture of the Special Forces soldier on horseback with his notebook computer has become symbolic of NCW, then an operation conducted two years later, but which has not received the attention it warrants, may yet assume much greater significance.

In the months leading up to the invasion of Iraq on 19 March 2003, a small group of Australian, American and British Special Forces won a remarkable victory. Their immediate objective was to ensure that western Iraq was free of Scud missiles that might have been fired at Jordan and Israel, thus dangerously broadening the pending war. Not only did the allied forces meet that objective, but also they effectively controlled about one-third of the territory of Iraq. According to the Chairman of the US Joint Chiefs of Staff, General Richard Myers, the key to that extraordinary achievement was the availability of air—surveillance, reconnaissance, information, and strike—24-hours a day, seven days a week, which was fully integrated with the action on the ground.<sup>13</sup> This little-known operation may represent the epitome of the 90-year history of air/land warfare.

The degree of inter-Service cooperation implicit in that achievement stands in stark contrast to the experience of the route packages in Vietnam. The point cannot be over-emphasised: organisational arrangements and inter-Service goodwill—that is, the basic components of effective communication—are probably more critical to our ability to conduct NCW than any high technology equipment. Vietnam provides a second salutary case study, this time involving Australia.

---

<sup>12</sup> Group Captain P.J. Criss, *Employing Smart Technology in Low Intensity Conflict*, Air Power Studies Centre Paper No. 6, Air Power Studies Centre, Fairbairn, August 1992.

<sup>13</sup> General Richard Myers, quoted in ‘US Push to Base Forces on our Soil’, *The Weekend Australian*, 17 January 2004, p. 001.

Prior to the Defence reorganisation directed by the newly-elected Whitlam Government in 1973 and conducted under the leadership of the then Secretary of the Department, the formidable Sir Arthur Tange, Australia's Navy, Army and Air Force were legally distinct entities, each with its own department and minister. While there was a Chairman of the Chiefs of Staff Committee, the incumbent could only coordinate and advise. He held no statutory authority to command and control anything. The three single Service boards were individually responsible to their respective ministers for exercising statutory authority over three separate organisations.

In 1965 (that is, before the Tange reorganisation) it had become apparent to the Australian Army that their existing commitment to the growing conflict in Vietnam might be increased to task force size, a change which would almost certainly demand the deployment of RAAF-operated helicopters, rotary wing capabilities having become an integral component of Western concepts of manoeuvre, reconnaissance and firepower. Consequently the Chief of the General Staff, Lieutenant General J.G.N. Wilton, had written to his Air Force counterpart, Air Marshal A.M. Murdoch, suggesting that the RAAF should send two Iroquois to Vietnam as an interim measure so the two Services could gain some early experience in the environment.<sup>14</sup> Preoccupied with the RAAF's efforts to introduce the Mirage fighter and acquire the F-111 bomber, Murdoch peremptorily dismissed Wilton's proposal. Given that Australia was already involved in the war in Vietnam, and that the acquisition of the Iroquois had in part been justified by the Army's requirements, Murdoch's response was, to say the least, extraordinary. Yet there was little Wilton could do, other than feel justifiably angry.

Once again the message is clear: it is almost impossible to overstate the importance of organisational culture as a principle of NCW. How can people network if they cannot or will not talk to each other?

Despite the acrimony caused in the 1970s and 1980s by the Tange reorganisation, the demolition of the insular, indeed selfish, single Service structures and outlooks that had facilitated attitudes like Murdoch's has been fundamental to the Australian Defence Force's progress, first, towards a genuine joint system; and presently, in its inexorable march towards an integrated, 'beyond joint' system.

In conclusion, like most things in life, the idea of network centric warfare is not new; and nor may it be applicable to every contingency. But by drawing on the continuing revolution in information technology, miniaturisation and precision, today's model of NCW promises an unparalleled level of situational awareness to those who master it.

Because the current model (if not the general concept) is so ambitious, there are no historical examples with which we can draw close parallels. But as this very brief history has attempted to show, there is any number of partial examples we can use to inform our progress.

---

<sup>14</sup> This episode is discussed in detail in Alan Stephens, *Going Solo: The Royal Australian Air Force 1946–1971*, Australian Government Publishing Service, Canberra, 1995, pp. 289–91.

History suggests that three separate but related tools hold the key to unlocking this potentially immensely powerful capability, and all have been visible in the constant evolution of the Western way of war since the start of the 20th century. The first is to fully exploit technology; the second is to establish the correct organisational structure; and the third is to build the essential institutional and personal cultures. All must be present; none can succeed without the others.

No nation has ever managed to construct a fully-integrated, three-dimensional, networked defence force, and in the next half-century most will find the challenge beyond them. But for those that succeed the rewards will be immense.

Lord Kitchener knew that.

\*\*\*\*\*

## ***DISCUSSION***

*A combined discussion period was held after Mr Samu Kainikara's presentation—see page 114.*

# **FUTURE OPTIONS FOR AUSTRALIAN AIR POWER**

**MR SANU KAINIKARA**

## **INTRODUCTION**

The intellectual response to the end of the Cold War was, if anything, inadequate to prepare the world for the emerging unipolar but multifarious international society. The response from most military thinkers was to focus on the so-called Revolution in Military Affairs, primarily driven by advances in technology, especially information technology. Although the threats that emerged after the events of September 11 were simmering below the surface for a number of years prior to the event, it was the catastrophic effects of the attack itself that forced the nations around the world to reassess the threats to global and national security. A salutary effect of this acceptance of an emerging and as yet unquantified threat, and our vulnerability to it, was to reinvigorate the intellectual debate in the analysis of the continuously changing nature of conflict.

There still exists a political thought process that adopting a broad concept of security will dilute military strength and the power base that it provides to the nation. Global politics and national security, however, cannot be separated even in the context of a narrow viewpoint of purely military security. The basic concept of security itself is complex and it is made more so by the necessity to take into account warfare in all aspects of security considerations. Warfare is a non-linear system in which inputs and outputs are not proportional, where cause and effect is not clearly evident, and it operates in an environment of unpredictability and constantly requires new methodologies to be successful.

The nature of conflict is continuously changing and this change permeates to the lower level of warfare reinforcing its unpredictable nature. In combination with the current fragile international security environment, this situation leads one to believe that the world is in a state of global transition. Unfortunately most of these transitions are destabilising in nature leading the international society headlong into chaos, confusion and conflict. The major transitions of this nature are taking place in social, economic, institutional, technological and informational spheres, each having its own sizeable impact on global security.

The destabilising influence of uncontrollable transition and unpredictability of emerging threats put enormous pressure on nation-states in their attempts to remain viable and relevant entities. Many respected analysts are of the opinion that the nation-state is a doomed enterprise and that only very large-scale organisations will survive the onslaught along with the non-state entities that have sprung to prominence in the recent past. National boundaries have been eroded equally by economic globalisation and transnational crime, while ethnic groups demand separate enclaves for themselves more vociferously than ever before.

It is from this uncertain base that future challenges have to be analysed and options to counter them developed. The age we live in now is full of contradictions and it can be said with some assurance that this trend will continue. However, it is preferable to stay ahead of unfolding events in order to ensure robust national security, or if not, at least be adaptive enough to respond credibly at the earliest. Staying ahead of events can best be achieved by anticipating the requirements of the future in time and initiating preventive actions in order to pre-adapt to evolving situations. These actions will also contribute to shaping the strategic environment to one's own advantage. Force projection capabilities will have to be modified and refined as an ongoing process for them to retain their relevance in the modern environment. The increased lead time required to field the desired equipment operationally that will in turn produce the necessary capability at the required quantum dictates that the future security environment can only be ignored at one's own peril.

Two fundamental questions need to be answered before any future options can be analysed in detail. First, what will the future security environment look like? Second, what is the percentage assurance of the veracity of such a prediction?

## **FUTURE SECURITY ENVIRONMENT**

Looking beyond the next ten years to define the future security environment is wrought with the very real risk of being completely wrong. There are no certainties involved in any of the situations that consume international conscience and, therefore, it can be assumed that at least some of the current trouble spots will have settled down. The corollary is that new areas of tension will likely emerge, as will new mechanisms for the adversary to create effects on us to get their way. However, despite the uncertainty, it is necessary to establish some kind of acceptable future scenarios to look at what the military forces can provide by way of assuring security of the nation. The closer these scenarios are to the actual one that unfolds, the easier it will be for the force to adapt to the emerging situation.

At the base level there has to be acceptance of a few clearly understandable and supportable assumptions. To consider the emerging security environment of the next 30 to 35 years, the following seven assumptions can be made with an acceptable amount of assurance.

- The United States will remain the primary superpower, although strategic challengers to its primacy will emerge, probably in Asia.
- Although the United States will continue its global engagement, it would have already withdrawn from the outer perimeters of its global commitments, indicating a growing reluctance to engage universally.
- The imbalance of global distribution of power will become more acute.
- Threats to national security will become increasingly borderless.
- Technology, especially military technology, will spread even more rapidly.

- Proliferation of Weapons of Mass Destruction (WMD) will continue, even perhaps at a faster pace than now.
- The 21st century will be an age of synthesis, where information technology will permit the combination of sciences to produce almost unimaginable outcomes.

The challenge to the primacy of the United States is most likely to emanate from the growing economic and military capabilities of China. The capabilities will not match those of the United States, but it is more than likely that China will tend to act the role of a second superpower sooner rather than later. This would have long-term strategic implications. The scaling back of its bases and garrisons in East Asia and withdrawal of US presence from other outer perimeters will be spurred by the increasing Chinese influence in the region. The United States will resort to a policy of selective global engagement.

While most of the assumptions that have been listed are strategic in nature, for this paper the spread of technology has special significance. The home computer was first unveiled in March 1977. Within the first two decades there were more than 18 million desktop computers in the United States alone! In the early 1990s, cellular phones were an expensive rarity. Today they are cheaper by an order of magnitude, more capable and ubiquitous even in developing nations. What is even more wondrous is that in the very near future high-speed wireless data transmission and space-based services promise to revolutionise the face of communications completely.

Computer and communications technology and the pace of their evolution are the core driving factors in a revolution in how people worldwide live, work and make war. These two capabilities are not merely convenient tools of the stock market, but form the backbone of a redundant and robust military command and control system. Three distinct trends are discernible in future technological development as a whole and applicable especially to the twin aspects of computing power and communications. First, proliferation of high-end military technology can be assumed to become a norm, rather than an exception, mainly because economic globalisation has made the trade in arms the most lucrative commercial activity. Second, with the increasing demand for commercial technology to be of a higher standard and redundancy, dual-use technology will see a quantum increase in capability, with significant security implications. Third, space-based capabilities will enhance communication networks in speed and volume of data, and also make low-cost, high-resolution spectral imagery available to all users.

Based on the assumptions and considering the current strategic environment, one can assume a spectrum of different global security scenarios. One end of the spectrum will be a rather mundane and evolutionary linear projection of today's world out to 2035. However, even in this scenario, change will be a constant factor, with the change being slight and embodied gradually. These changes will be more in the form of altering regional groupings of countries and non-state agencies, and the decisive influence they exert in certain areas of the world. It is even possible that the change itself may go unnoticed except when it erupts violently into prominence sporadically. The positive side of this scenario is that even though the power equation changes constantly, there is very limited violent upheaval associated with it in the medium term.

The other end of the spectrum is one of violent confrontations, anarchy and chaos. The number of 'failed states', with all the destabilisation of the region that it entails, will be on the rise. The most likely progression of events in this scenario is extreme and rapid proliferation of WMD as more and more states opt to obtain these as insurance against the increasing dangers in their region. This scenario is more likely to produce the strategic challenge to the world leadership of the United States that was alluded to earlier.

Irrespective of the overall state of the global security environment and the direction of its potential shifts, some trends are discernible today that will continue to hold steady. First, Europe will continue to become a more articulate economic and political power while developing into two clear and opposing groups, the European Union and Russia. This bipolarity will create palpable tensions and a clearly unstable region in Central Europe. Second, the Middle East will see an increase in trans-border interference in internal security matters. The increased volatility in the security environment in the region will spill over to Europe and Asia in a widening spiral of instability. Third, while the Asia-Pacific region will emerge as the most important concentration of world economic powers, it will also remain turbulent and insecure because of the changing external environment. However, China and Japan will clearly be the economic leaders in the region, operating in a state of uneasy acceptance of each other.

The veracity of the above assessment regarding the shape of the future world lies in the uncertainty that it predicts. This uncertainty is centred around the certainties that have also been predicted. Essentially the world that one has to look at when considering the options available for the effective employment of air power in support of national security imperatives is one with a somewhat predictable kernel within a complex and unpredictable shell. In the global security environment there will always be tangibles and intangibles, as well as constants and constantly changing ephemeral scenarios that belie its visible peaceful exterior. The future holds surprises of great magnitude for even the most prepared of forces leading one to ask what, then, is the answer to this rigmarole? The answer lies in preparing for the unfathomable to the extent that the predictable changes permit and being as close to the unpredictable as possible.

## **TRANSFORMATION IN THE CONDUCT OF WARFARE**

Military forces now need to respond to a wider range of potential threats as compared to half a century back and the rate at which the range is increasing will be exponentially higher in the next 50 years. This makes military planning more uncertain than ever before. The increased lead time required to field a capability operationally in the emerging high-tech environment increases the uncertainty to an almost unacceptable level. Maintaining the status quo indefinitely has never been an option for a military force, but the Cold War provided military planners with a false sense of security regarding force structures. Today's world is inherently more dynamic and the challenge now is to ensure that the force is capable of adapting at a strategically useful rate while retaining effective capability.

There is no doubt that we are now firmly in the Information Age and that traditional doctrine, strategy, tactics and command and control processes are no longer sufficient.

This has necessitated a transformation in the conduct of war and other military operations to encompass the effective utilisation of technology-aided capabilities. While all force projection capabilities need to be cognisant of this need, it is in the employment of air power that an absence of this awareness can be felt in an unambiguous and immediate manner. It is certain that any conflict in the future will be joint and that the relative 'jointness' will depend entirely on the force's adoption of emerging technologies and inherent interoperability. Air power, because of its characteristics, will become the binding factor in such an enabled force.

All through history, chaos and calamity have been unchanging characteristics of war. But the defining characteristic of warfare in the information age is the technological capacity to ensure near real-time coordination of numerous weapon systems over great distances, thereby producing effects far greater than was possible before. The primary effect of such a situation is that there are no clearly defined battlefields or battlespace anymore. This is the main reason why air power that has always operated beyond the threshold of the traditional battlefield is well placed to absorb and exploit this concept.

## **THE FUTURE OF AIR POWER**

You can only predict things after they have happened.

– Eugene Ionesco

The development opportunities available to air forces around the world depend primarily on the basic security stance of the nation. Even though it is the future of air power that is being discussed, the fact that there are clearly two types of air power in the world today—that of the United States and the rest—has to be understood. This paper confines itself to looking at the future of air power in terms of options available to an air force that operates under a certain amount of realistic resource constraints.

### **Assumptions**

As with looking at the future scenario that will emerge, it is necessary to make a few initial assumptions in order to ensure that a fairly robust foundation is available to base the understanding of changes and to compare them with contemporary notions of future possibilities. The assumptions are as follows:

- The world will remain an uncertain place and it will be impossible to predict the nature and timing of crises.
- Air power is inherently 'joint' and will continue to be highly prized for its characteristics of flexibility and ubiquity.
- Technology is the driving force in the dynamic changes that are taking place in warfighting capabilities, but it is still not capable of providing all the answers to emerging challenges.
- Human and social factors will continue to be vital to the achievement of the desired end-state.

- Political expectations, legal constraints and funding limitations will increase the pressure on military forces to deliver more with less, making the application of military force a challenge.

### **Ongoing Transformation**

While analysing the most logical way in which air power would develop, the first area that has to be studied is the ongoing transformation that is already taking place in the application and appreciation of air power. There are a number of factors that influence this process. First, the accuracy of forward thinking has improved dramatically in the past decade with the application of a number of technologically advanced tools. Second, military forces around the world are now more aware of the necessity to have adaptive and dynamic doctrine to underpin all their actions. The combination of these two factors provides an increased predictive awareness to the planning phase of all operations.

Third, technology-aided intelligence fusion and the concept, as well as the capability, to carry out time sensitive targeting is one of the cornerstones of this ongoing transformation. Increased predictive awareness combined with accurate intelligence and the ability to carry out time sensitive targeting provides air power with the capability to alter the character, scope and tempo of all operations. Fourth, air power now has an improved capability to combine timeliness, reach and precision, much more than ever before. The overall effect of the four factors when combined optimally is to create a situation wherein the decision-making cycle, the classic OODA loop, can be compressed almost to real-time capability.

### **Emerging Threats and Air Power Responses**

Future threat trends indicate that there will be a movement away from conventional attacks on traditional forces. When faced with technologically advanced forces the adversaries will not try to match force with force. Instead, the attempt will be to resort to the equalising force of asymmetry by relying on classic terrorism and guerrilla tactics, especially in the urban environment. There will also be increased assault on cyber networks at nodal points in an effort to paralyse the broader operational capability of a nation. This will be the adversary's version of effects-based operations, where the attempt will be to neutralise the advantage that a greater power has in terms of the capability to bring all its might to bear.

Nano-technology is another emerging area that will be used by adversaries wanting to create as much asymmetry as possible and to neutralise the technological advantage that is inherent in developed air power capabilities. In this sphere, capabilities are being fielded that can create numerous tiny, cheap threats which in turn have the capacity to overwhelm even the most sophisticated air defence systems. Such a swarming technique, commonly available, will threaten the fundamental structure of a defensive response. It may make vastly more expensive and complex defensive systems obsolete overnight.

Air power responses to these threats have to be carefully graded. Most of the air forces around the world are grappling with the problem of block obsolescence of legacy systems. The few legacy systems that are still capable of producing the desired

effect are becoming far too expensive to maintain and operate with adequate efficacy. It can be said with a great deal of assurance that continuing to rely on the legacy systems will not be a viable option for a 21st century air force. Under these circumstances it becomes even more important to ensure that the systems that are being introduced are capable of adapting and responding to the emergent threat scenario.

The primary responsibility for an air force in the future will be persistent battlespace dominance to provide an umbrella for surface operations. Battlespace dominance will be achieved through a combination of disparate yet interconnected capabilities. These capabilities would involve offensive actions necessary to neutralise enemy threats while obtaining and maintaining control of the air, and the need for constant and continuous intelligence gathering and surveillance. These capabilities will require platforms that are capable of carrying the systems that can produce the desired effects. The future will see a combination of inhabited and uninhabited platforms operating both independently and in tandem with each other. They would be stealthy, with enhanced endurance, reach and flexibility. These platforms will routinely perform high altitude, long-duration missions to improve time sensitive targeting capability, as well as persistence in surveillance. The combination will be cost-effective and produce sustainable capabilities because of the larger number of systems that can be made available at any given time.

The systems that these platforms will carry will also be technologically far more advanced than even the most sophisticated systems in use today. The trend is visible in the research and development currently taking place in these areas. Directed energy weapons that would almost completely eliminate collateral damage are likely to be fielded operationally in the near future. Refinement of this system to make it possible for smaller platforms to carry and employ it can also be expected in the not so distant future. Another emerging attack technology concerns non-lethal solutions. Currently there is no comprehensive understanding of this developing system, and it is likely to create a furore in the human rights groups when utilised. However, there is no denying the fact that a number of developments indicate the willingness of military forces to employ these weapons when they are made available.

The air power response to emerging threats that has been outlined is based on the understanding that information age warfare will be dominated by the force that has better situational awareness. Situational awareness is almost completely dependent on data transfer rate and redundancy. The closer it is to real-time the better the situational awareness. Greater awareness translates to an increased speed of response permitting the force to operate inside the OODA loop of the adversary. In combination with the speed of reaction, this ability will also bring with it the capability to control the tempo of all operations. The essence of information age warfare is the leveraging of one's own situational awareness to an extent wherein the enemy is overwhelmed into capitulation.

### **Air Power Challenges in the Information Age**

There will be four major challenges that will have to be addressed for air power capabilities to be effective. First, the unpredictable nature and timing of all emerging crises will give inadequate warning time for preparation. The air force will be forced

to go into the fight with existing doctrine, preparedness and equipment. The primary need to get the capability development process as accurate as possible is therefore reinforced. In addition, flexible thinking and adaptation of capabilities to achieve the desired effect will become cardinal virtues.

Second, the impact of artificial intelligence, which is bound to mature in the future, will be felt not only when the political and legal aspects are considered, but will have to be taken into account in deciding the way forward for command and control issues. The challenge will be to combine human and artificial intelligence effectively to shorten the decision-making chain and to delineate their individual positions within the complex system. This will require a more than ordinary understanding of both human factors as well as endemic system issues.

Third, is the now accepted capacity of air power to have global reach and, therefore, the capability for rapid entry into crisis areas, which will have to be balanced with the quantum of capability that can be so deployed. This amounts to ensuring the availability of more than adequate persistence, in accordance with higher directions, to support the rapidity, reach and precision that are already inherent in air power.

The fourth challenge is perhaps the most difficult to overcome. Information superiority is the basis on which entire campaigns are built, fought and won. The increasing availability of space-based commercial assets to friend and foe alike makes the obtaining of such assured superiority very difficult. The edge in assuring information superiority hinges on unhindered access to flexible, affordable and jam-proof, space-based surveillance and communication assets. Given the current trend, this is a tall order. The future might see the use of high-flying, long-endurance UAVs as viable alternatives, although the limitations on bandwidth will continue to pose a formidable challenge. This situation will only get exacerbated in the future and will form a constraining factor in the unlimited application of network centric warfare.

### **Future Air Power Characteristics and Roles**

The future characteristics of air power will be more complex than the current list. They will cover a larger spectrum although there will only be four clearly identifiable ones. The first will be the primacy of air power assets in their ability to ensure information superiority. Information superiority in the future will only be possible with adequate air and space assets that have great redundancy and robustness. The second will be the ability to shape the battlespace, both in high and low intensity conflicts. This characteristic will be the overriding and controlling factor in the employment of air power assets and has implications for all operations. The third characteristic will be that an effective air force will need to be both balanced and versatile. The balance in capability would depend on the priorities assigned to the force by national security considerations, but versatility in whatever form the force is structured would be a constant factor. Fourth will be the ability to provide rapid and overwhelming response to all emerging threat situations with simultaneous, multi-pronged and precise attacks on identified centres of gravity.

The future air power roles that emerge will be strike, command of the air, airlift and enabling operations. The competencies of reach enhanced by air-to-air refuelling, payload with increased effectiveness, and precision that provides discrimination and

timeliness in target neutralisation, gives air power strike capabilities that create strategic effects with minimum effort. This has created a perceptible doctrinal shift in the employment of air power that will continue to make strike the primary role. This is not to suggest that command of the air, till now the *raison d'être* of air forces, has become a redundant role. What has emerged and will get sanctified in the future is the capability of air forces to strike at will, and command of the air becomes a requisite for the successful completion of that mission like any other land or maritime mission. Currently available air power capabilities bring to focus the interdependence between strike and command of the air in much the same way that Douhet envisaged in the 1920s. The difference is that Douhet's concepts were dismissed as wishful thinking, whereas today technology provides the wherewithal to prove the claims right. The question to be asked is how this doctrinal shift towards reliance on air strike will impact the overall warfighting doctrine at the highest level?

The responsiveness of airlift to emerging situations and the capability to carry out concurrent operations by simultaneous deployments will make large volume, one-time airlift a coveted capability. In consonance with the inherent characteristics of Special Forces, the speed, tempo and precision that can be achieved by timely and adequate airlift capabilities increases by a magnitude. It can be safely assumed that air power will be required to provide airlift support for a variety of operations on a continuous basis well into the future.

Enabling operations are all support missions that enable the smooth conduct of strike, command of the air and airlift. It is in this role that the impact of space-based capabilities will be felt the most, at least in the near to medium term. The increasing reliance on space-based assets for communications and ISR would have to be tempered with their availability as well as cost considerations. This is even more painfully obvious in the case of smaller air forces where the need to understand resource allocation priorities will become a vital factor in long-term planning.

### **Future Options for Australian Air Power**

There are two issues that will influence the direction that any air force would take in its medium to long-term development. The first is resource-related. The longer gestation period to field any capability and the longer service life of assets combine to ensure that the only cost-effective way to maintain the required proficiency would be to adopt an incremental upgrade program rather than whole-of-system replacement. The second is the absolute necessity to be networked and the attendant risk it brings. Over reliance on technology can lead to the human factor either being ignored or left out of the loop completely, with gravely detrimental effects. Networks are also vulnerable to a range of direct and indirect attacks that can disrupt information sharing and affect timely decision implementation. The integrity of networks will also be a major issue, especially when operating in coalitions.

While looking at options available to Australian air power to remain effective and relevant it has to be understood that some decisions that have already been made regarding the acquisition of capabilities/platforms for the future will have a more than salutary impact on air combat capability. It is almost certain that the Joint Strike Fighter (JSF) will be introduced into the inventory in another decade or so. This platform is intended to be the mainstay of the RAAF for both air combat and strike

capabilities for 30 years or more from its induction. What future planners will have to take into account while juggling the capability spectrum is the very real chance that the JSF, or which ever platform is inducted, may not be able to provide the desired capability for the calculated time period.

There are a host of disruptive technologies that are nearing maturity—robotics, genetics, smart materials, nano-technology—all fully capable of completely transforming military operations in the next 15 or so years. A strategy that completely negates any kind of flexibility would therefore be self-defeating. Future planning will have to be cognisant of this factor and will need to constantly create windows of opportunity to ensure that the Air Force possesses effective and relevant capabilities.

From an Australian perspective, fleet size and therefore quantum of capability will be determined by the size of the RAAF. In order to leverage the small force to deliver more than its weight, the air power elements would have to be looked at in a ‘system of systems’ methodology. This would ensure that the force produces a total and balanced effect rather than disparate group of effects. Platform-centricity will have to be replaced by networked whole systems producing the desired effects. Failure in this attempt will move the RAAF to the sidelines and subsequent obscurity. Capability oriented planning and execution will have to be adopted as the key imperative.

Air power will have to embrace the concept of both conventional and uninhabited air vehicles operating in conjunction with each other to provide the necessary capability. This would require an increased understanding and reliance on artificial intelligence. Purely machine-to-machine interaction will reduce the sensor-to-shooter time frame to milliseconds. The advantage is that information processing for the human ‘decision-maker’ will become extremely fast, closing the OODA loop further.

Australia will have to nurture evolving aerospace technologies, such as the hypersonic scram jet that is undergoing trials, to remain at the vanguard of developments that will facilitate effective employment of air power. Space applications will also have to be carefully woven into everyday operational concepts so that they become an integral part of Air Force operations. The long-term future will, no doubt, see the weaponisation of space and the RAAF needs to be constantly aware of this. This aspect is fraught with delicate legal and moral issues that will also need careful consideration.

At the tactical level, the need currently being perceived for organic offensive air power capabilities will diminish. Slow moving platforms, like the attack helicopters, will become even more vulnerable than they currently are in a technology-empowered battlespace. Joint operations of the ADF will have become more seamless and, therefore, air assets will be available on call to support surface forces. A combination of factors—acute resource constraints, enhanced precision and lethality of air weapons, casualty-aversion and real-time networking—will ensure that battlefield offensive strikes are conducted on an as required basis mainly by centrally controlled uninhabited air vehicles. Air power in the future ADF will have to adhere to the concept of unity of command because of necessity.

## **CONCLUSION**

Air power will transition to long-range strike capabilities using a number of sensors, systems and decision-making tools that provides instantaneous information management capabilities. The core competencies that air forces will be relied upon to provide in a joint environment will be reach, payload, precision and flexibility. For even the smallest of air forces to remain relevant it will be necessary to be able to have rapid, sustainable and versatile deployability. This will have to be achieved within an ever-shrinking share of the available resources.

The future will always hold challenges to air forces, both in terms of rapidly changing threats and uncertain capability development processes. The situation will be further exacerbated by five enduring and universal factors that will always affect future development. These factors are:

- the size of the military budget, which will always be finite;
- contemporary political perceptions of major threats to national security;
- the character of the Government, which will determine the reaction of the nation to both covert and overt threats;
- the level of aviation technology that will form the basis for maintaining the technological edge; and
- the competence of the military leadership, which will be complex at all levels.

Australian air power will have to face a future that will bring doctrinal changes and challenges to the fore at random, and with varying degrees of urgency. It will be a wise and competent air force that will keep a constant watch on the changing scenario and adapt its doctrine to face the challenges of the future. This is the only sure way to contribute to national security and remain relevant. For an air force, like the RAAF, any other option is bound to bring it into a downward spiral of diminishing capabilities leading to an uncertain future.

This is the key point: the effective employment of air and space power has to do not so much with airplanes and missiles and engineering as with thinking and attitude and imagination.

– General Merrill A. McPeack

## **BIBLIOGRAPHY**

Alberts, David S. and Czerwinski, Thomas J. (eds.), *Complexity, Global Politics, and National Security*, Command Control and Research Program (CCRP) Publications Series, Washington DC, 1997.

Alberts, David S., Garstka, John J., Hayes Richard E. and Signori, David A. (eds.), *Understanding Information Age Warfare*, Command Control and Research Program (CCRP) Publications Series, Washington DC, 2001.

Alberts, David S. and Hayes, Richard E., *Power to the Edge: Command and Control in the Information Age*, Command Control and Research Program (CCRP) Publications Series, Washington DC, 2003.

Kainikara, Sanu, 'Air Power in the Protection of Territorial Areas', Presentation at the Philippine Air Force Air Power Symposium, Manila, 6 July 2004.

Khalizad, Zalmay and Lesser, Ian O. (eds.), *Sources of Conflict in the 21st Century*, RAND, Santa Monica CA, 1998.

Scales, Jr, Major General Robert H., *Future Warfare*, Strategic Studies Institute, US Army War College, Carlisle Barracks PA, 1999.

ADDP–D.3.1, *Enabling Future Warfighting: Network Centric Warfare*, Defence Publishing Service, Canberra, 2004.

\*\*\*\*\*

## ***DISCUSSION***

*(A combined discussion period was held involving  
Dr Alan Stephens and Mr Sanu Kainikara.)*

*Mr David McIlroy (Air Force Scientific Adviser – Defence Science and Technology Organisation):* A question for Sanu Kainikara. I was intrigued by the sensor-to-shooter millisecond time scale because, surely, that removes the 'Orient' and 'Decide' component from the OODA loop, divorcing the commander completely from the equation. That's a huge cultural leap of faith and a huge risk, surely, to the conduct of operations. If you are not sure what you're seeing, you can't afford to shoot almost instantaneously, which is the way I took your comment. I'm interested in exploring that one a bit further.

*Mr Kainikara:* hanks David. What I was getting at is that we physically may not be seeing something but the way ISR capabilities are developing and the way in which artificial intelligence is being slowly incorporated into the cycle of the sensor, decision-making and shooting, it's really apparent that in say the next 25 or 30 years time the strike that will take place will be almost instantaneous and it will be definitely reliant on artificial intelligence, with maybe a diminishing amount of human decision-making involved in most of the cases. I'm not saying that it would take place in all cases. I think the first step that has been taken is creating these kill boxes, where anything that is inside that box can be struck without really having to check on its friend or foe status. I think that is going to be progressed further to the

extent where artificial intelligence itself will make the decision and action will take place in a time scale approaching milliseconds. That's what I was referring to.

*Air Vice-Marshal Eric Stephenson (RAAF Ret'd):* A historical comment for Alan Stephens. I was a navigator on Lancasters in Bomber Command in World War II. Our networking was curious in many ways but it was quite efficient. For example, an all-'Lanc' attack would be about 350 aircraft; that's 20 squadrons. We would be given a rendezvous point, usually off the Dutch coast, and we would be given the track to target. That attack would probably be in three waves; the first wave would be about three minutes, the second about three minutes and the third about three minutes, so as to concentrate the ultimate attack. We would be given a track and we would be asked to keep to within 2½ miles of that track. Furthermore, you would be given an operational height and you were expected to keep within 500 feet above or below that. Now, 350 'Lancs' going through that little channel would leave a hell of a lot of airstreams and every once in while you would hit a bump, which meant that you were crossing the airstream of a 'Lanc' in front of you. One of our navigational aids was every couple or three minutes you expected to have a bump. If the bump nearly turned you upside down, you were too dammed close! You had to do something about it. If, on the other hand, it was a gentle one, it was reassuring that you were staying within the block, and that was one of our navigational aids.

*Squadron Leader Grant Herrmann (RAAF – Training Aircraft Systems Program Office):* I've heard about directed energy weapons but the new weapon I heard about this morning was nano-technology. I was wondering what advances or what kind of applications you see taking nano-technology weapons taking. How will we be attacked in the future through nano-technology?

*Mr Kainikara:* I wouldn't say that nano-technology at the moment is in its infancy but probably is in its childhood. What we envisage is that, it being extremely cheap, it would be able to produce a large number of targets that could be used in what is being termed as a 'swarming' technique, where almost all your air defences would be saturated and once your air defences are saturated then the actual strikes can take place by other means. The nano-technology or the smaller robotics are not the ones that will actually do the strike—they would not be very effective—but the idea is to overwhelm the air defences with this technology and then send in the strike when you have no defences left. As I said, it's still in its childhood. It probably will mature in the next 10 to 15 years, and a great deal of work is being done all over the world on it.

*Wing Commander Paul Pappas (RAAF – Capability Development Group):* From a historical perspective, the military has always been at the forefront of technology development, and that held true probably until about 30 years ago. The assumption that I didn't see discussed in Sanu Kainikara's presentation was the issue that we are all assuming that these networks will be available for us in the levels and bandwidths that we're predicting we might need. The issue that I see is that the civilian use of their own networks and the electromagnetic spectrum is possibly increasing at a far faster rate than what we are predicting we may need. So the question I've got is, as a military organisation, how can we ensure that we actually have access to that spectrum, to the bandwidth that we need, if we only need it occasionally but will need it wherever we want to be able to use it?

*Mr Kainikara:* The only answer to that is to make sure that we have a whole-of-government approach to this in the sense that, as and when required, the military has to be given the bandwidth and the capabilities that it requires. We as an organisation by ourselves will not be able to ensure that, neither do we have the resources or the capacity to do that. As a future concept what we have to look at is making sure that a certain dedicated bandwidth and capability is provided to us on an as required basis—something similar to what we are doing with larger airlift capabilities, which we may not require on regular basis but would require in spurts, and what we are doing is to try to outsource it, try to get resources from that sector. The only thing is when you talk about the bandwidth it would have to be dedicated availability. That's the only way forward; we cannot hope to keep something locked up for that long.

# **NETWORK CENTRIC OPERATIONS AND MODULAR SYSTEMS**

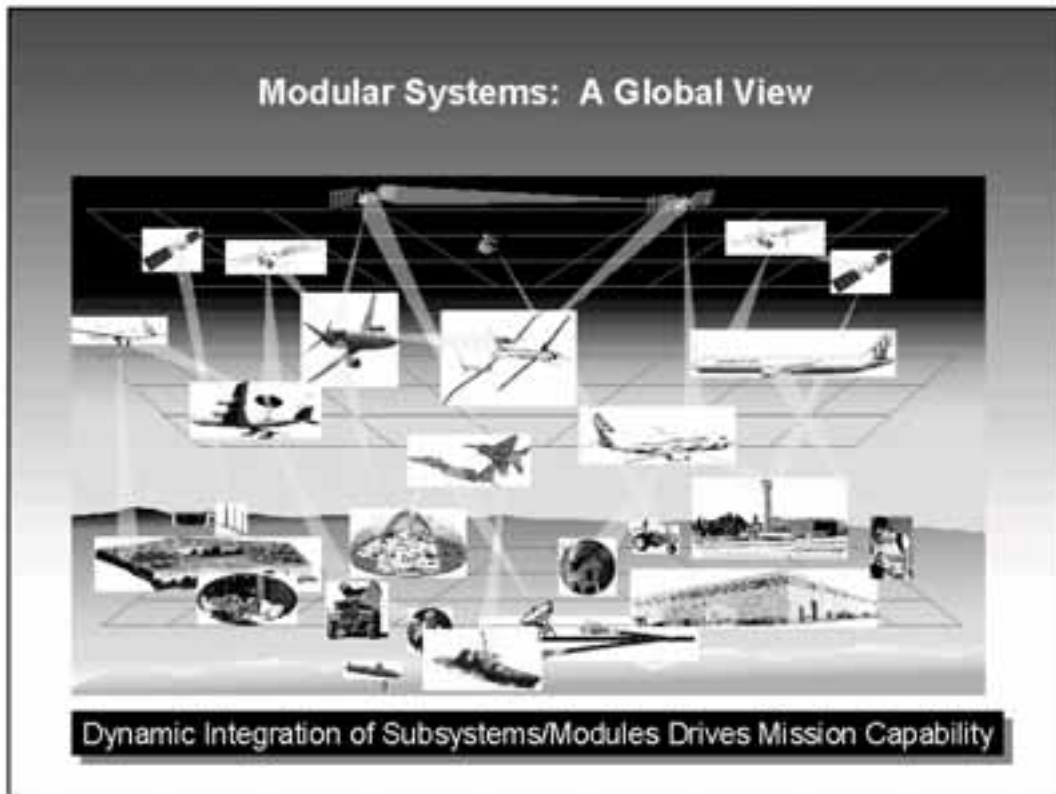
**LIEUTENANT GENERAL CARL O'BERRY (USAF,  
RETIRED)**

It is always interesting to think about how a mere engineer has the temerity to walk to the stage following such intellectual giants as I have heard speaking here this morning. I will not even try and match the vernacular and the profundity of that level of thinking; you will just have to put up with me as a raggedy engineer trying to get a message across. I have two rules of engagement that apply to most of what I do. One of them is: do not attribute to malice that which is accomplished through ignorance. A corollary to that of course is, do not mistake malice for ignorance. The second is: you can get almost anything done as long as you do not care who gets the credit for it.

We have heard a great deal from many people over the last two days about network centric operations, and almost without exception the slides that go up and the discourse that ensues is incredibly complex. Lieutenant General Hurd, a contemporary of mine and an old friend, speaking about network centric operations is quite a shock to me. But you look at the slides he put up and you might say, 'How in the world are we ever going to get control of this? How are we going to translate that set of requirements for things to interact, at the level that he described, into reality?' Well, simplicity perhaps does not apply always, but physics does. So I thought it might be useful this morning to talk about the 'how' of this. Not to insult your intelligence by being too shallow in the approach to it, but perhaps to get you to think a little bit about what the art of the possible might really be. I will try to avoid the 'A' word [architecture] too much. If I overstep my bounds on that score, I am sure you will chastise me for it.

Let me preface this with a couple of thoughts. Number one, Joint Vision 2020 to me is almost a contradiction in terms. How you establish today what the world is going to look like in 2020 is beyond my comprehension. Because the technology is advancing so fast, we have to find a way to deal with increasingly short cycles of technology. So whatever we do, the foundation that we build to accommodate the requirements of information systems and network centric technology must be one that is amenable to the insertion of new technology as it develops. Joint Vision 2020, to me, is a vanishing point on the horizon—in exactly the same sense that a draftsman puts a perspective point on his paper horizon and draws things consistent with that vanishing point. That is, whatever you do here in the near part of the drawing is going to be aimed at that vanishing point—there may be more than one but, in general, we talk about one in the simplistic way—so that everything going into the drawing is consistent with that vanishing point. Let us think about Joint Vision 2020 and its like in other venues as that kind of vanishing point. There are myriad opportunities to approach various operational requirements with technology; so many, in fact, that from a business perspective I have become convinced that you can be overcome by insurmountable opportunity. That is an old *Pogo* cartoon saying, and I believe it to be

pretty much a true and useful thought perspective today. So let us talk about this in terms of some rules that one might apply and try coming to grips with all of this.



**Figure 1 – Modular Systems: A Global View**

Figure 1, proceeding from left to right, shows schematically almost everything you can think of, from military to industrial—in fact, all the way to the consumer venue—that might be addressed more effectively through networking the tools of one’s trade, and there are many good reasons for that. We began looking at network centric operations as primarily the venue of the military. Perhaps, that’s because there is an inclination for us to start with that which is familiar to us, and in the integrated defence systems business the military customer was the driving focal point for defence industries at the beginning. But I want to make this picture perhaps a little bit more explanatory in the light of questions that I have heard over the last couple of days about bandwidth, among other concerns. How do you get all these things done within the constraints of current bandwidth and other resource limitations?

I would suggest to you that if we could establish as rule of engagement number one that we get rid of the classic telecommunications model with which we have been born and raised, bandwidth might become a non-issue. That classical way of thinking addresses an analogue environment, where everything must be connected in some fashion in order to exchange data. In the digital world that is simply not true. As a matter of fact, let us go back now a few years to the establishment of the Ethernet and the guy who did that, Bob Metcalfe, who is one of the most brilliant engineers that I know, whose concern about bandwidth began to diminish very substantially as he began to examine what digital technology is all about. Let us think about the environment that you have heard described in the last couple of days in that light. For

the most part, we have been concerned about just bringing myriad things into the network and connecting them in some fashion. The way I tend to view that is: let us bring myriad things into the network, but let us make every one of them an element of the network infrastructure so that, regardless of what their primary purpose is, each of them is first and foremost a ‘packet router’. Each of them brings an infrastructure element into the environment. They are not connected—I think of them as richly disconnected. They have no need to be ‘connected’, in the classical sense; they need but momentary access to the ports provided by other devices in order to pass data packets. And if packets coming to them, for whatever reason, are not destined for them or their venue, they simply pass them on to another available port. The ports are in motion all the time, so it is not the same ports that enable packet passage for one transaction or another. The idea in this picture (Figure 1) is to graphically portray a constantly moving, agile beam distribution instead of the zigzags normally used to suggest an RF connection from one node to one another. In other words, agile sweeping beams, on lots of devices, concentrate data exchange energy in directional, fast and highly efficient sweeps over the operational space, allowing packets to flow between the various elements executing the operational direction of commanders or other decision-makers in this space. The dynamic integration of these subsystems drives what we refer to today as integrated mission capability. Incidentally, nothing in the picture is intended to be exempt from this proposition. So what does it take to make this vision a reality?

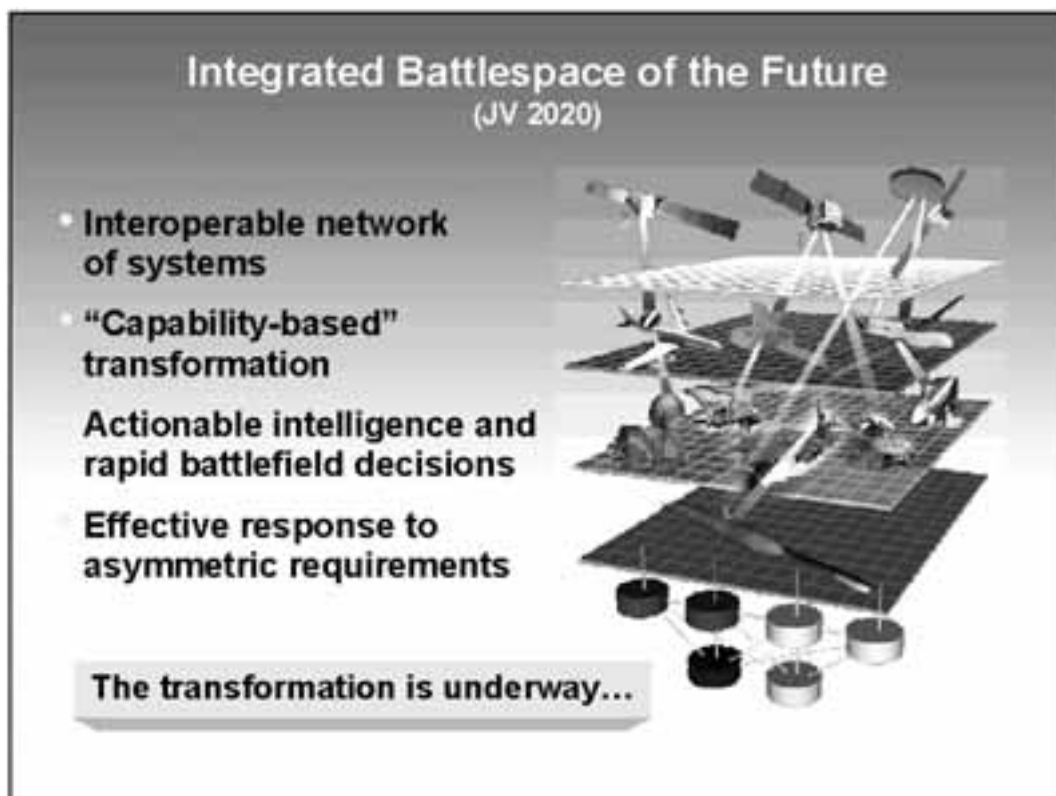
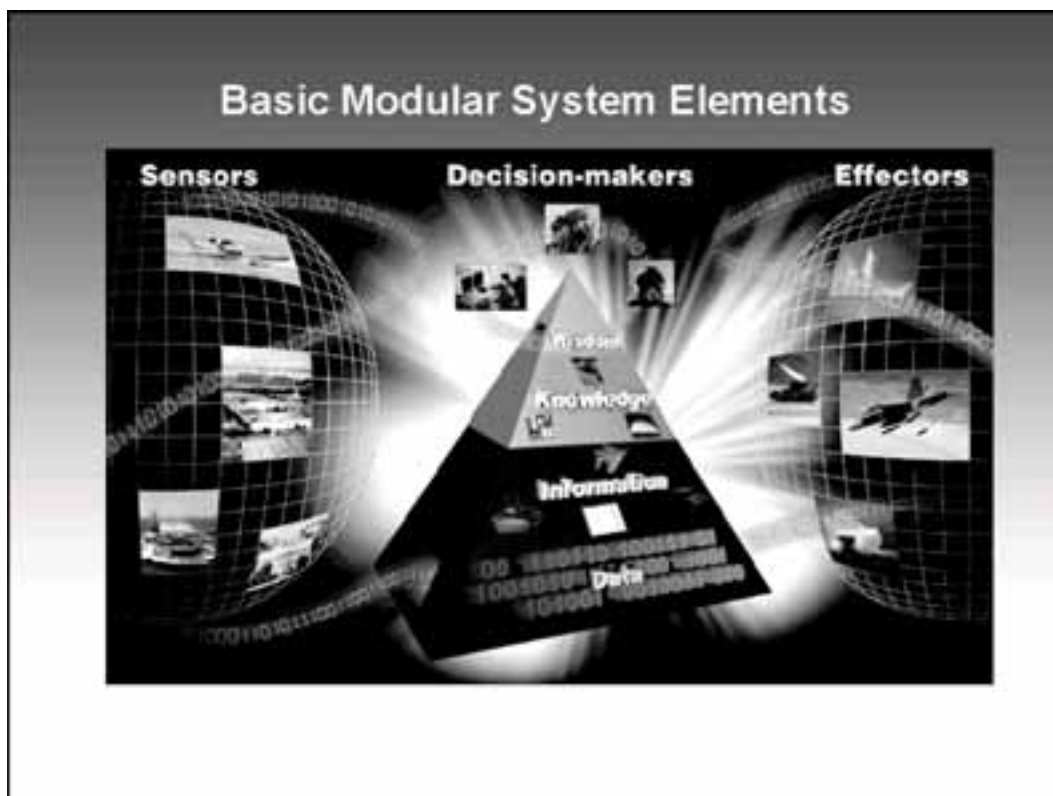


Figure 2 – Integrated Battlespace of the Future

Well, as suggested in Figure 2, think of the operational field first of all as an interoperable network of systems. There is a certain minimum level of interoperability that must be associated with every single object in the environment, regardless of its primary function. Second, we need to educate ourselves to change our focus to a

capability-based transformation to supplant the current view that suggests we have got to go out and capture all the bandwidth in the universe in order to accommodate it. The current-model requirements of a single Army Division suggest there is not enough bandwidth in the solar system to support its typical mission; hence every operational plan must be constructed in the face of major bandwidth limitations. Thirdly, when we talk about ‘actionable intelligence,’ we are talking about the capability for persistent intelligence, surveillance and reconnaissance (ISR) in the operational space—those kinds of things that help to formulate viable options for commanders to interact and respond to events. Finally, the response to asymmetric requirements has to be asymmetric in itself. We are fairly well convinced that transformation towards that vision is solidly underway. You have heard that from lots of speakers up to his point and so I am certainly not here to argue that point. But let me simplify all this. I do not personally care from my perspective what the object is that we are dealing with in a particular instance on the digital battlefield, or the integrated battlespace or the integrated medical space or the integrated ‘any’ space.

There are three classes of objects that I am concerned about, as shown in Figure 3.



**Figure 3 – Basic Modular System Elements**

The first is objects that gather or provide data in one form or another; they can be active sensors, they can be registered databases and so on. The second is the cognitive element of all this; that kind of object can be either man or machine depending on what level of comfort particular individuals have with regard to allowing machines to make decisions. Finally, the effector objects that are simply the things that cause some event to be addressed in some way that you define. Let us look at this in the military context then and think about what that sort of construct might look like.



Figure 4 – Integrated Battlespace

First of all, arrayed around the top of the left-hand side of Figure 4 are the objects that I refer to as sources. They require an interface with some sort of communications medium that allows that data to flow into the network and thence to the cognitive objects for which it is intended. There is processing activity that takes place in that context which drives a situational awareness information flow and aids decisions about options that are given to the forces to execute (effector objects). You could divide the various operational elements associated with that process into whatever form you would like but I have chosen, for want of a better way of doing it, to think about it as the communications function, intelligence and surveillance and reconnaissance function, global situational awareness function (ie. command and control) and, finally, an integrated command and control system that supports that process. Incidentally, I do not expect everyone, regardless of the size of their forces or complexity of their missions, to be as global in their outlook as we have to be in the United States. This is the product of an increasingly global mission that we see from the United States perspective. We do not know where the next crisis will require the application of our forces. We know that we are an increasingly expeditionary force, and that the capabilities of all military Services must operate jointly to accommodate the requirements to be addressed, wherever on (or off) the planet events might dictate.

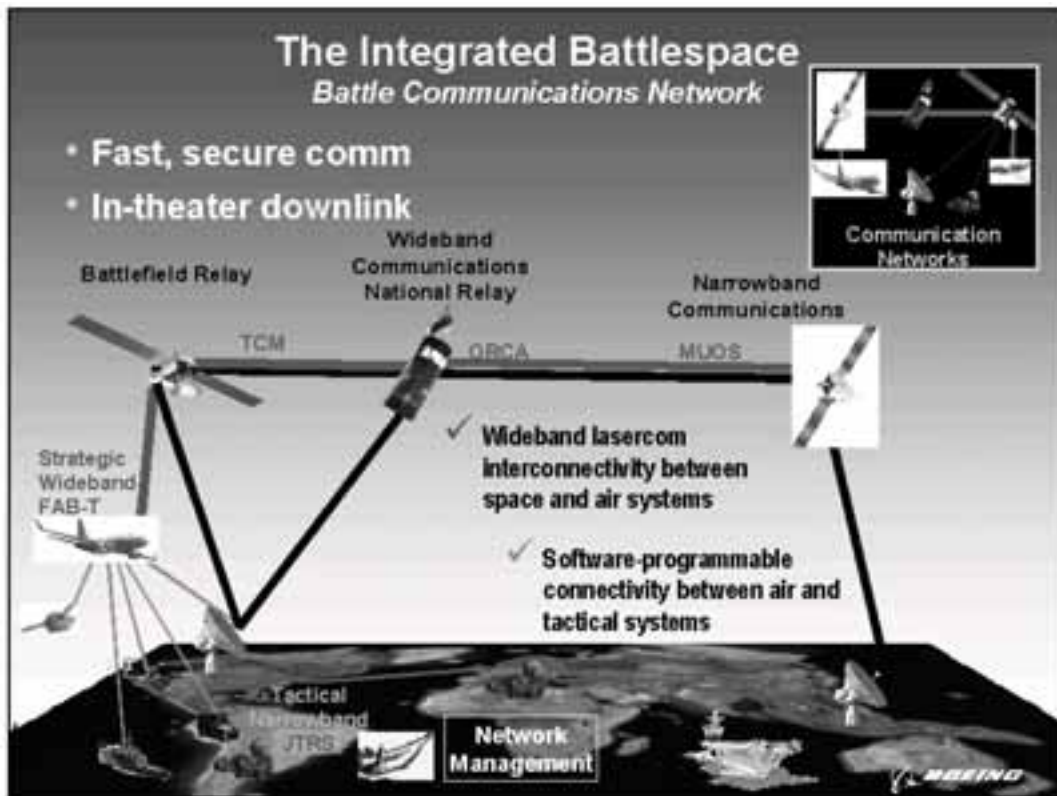


Figure 5 – The Integrated Battlespace: Battle Communications Network

That being the case let us think first about orbital platforms. Figure 5 represents a collection of such objects. The way we have historically treated those, using the classic model that I referred to earlier, is that they are monuments to somebody's genius, each and every one of them. They were typically not designed to interact with one another. In fact, we often times do not even know that they are there. One of the classic remarks that I heard during the first Persian Gulf War, when I was the J6 at US Space Command, was from a guy named Horner who ran the air war over there. Horner, who is not the most elegant guy that I ever heard but very colourful and effective in his communication, nonetheless, said (after some filtering), 'You're just not giving me enough bandwidth'. I said, 'You're probably right in the absolute sense, but I suspect that since you're a fighter pilot somebody told you to say that because you'd have never thought of it by yourself. And valid though the complaint might be, I think you're wasting about two thirds of the bandwidth you have available to you. I will try to provide you with more; but there is a limit to what I can do here.' The point that I was trying to make is that we were locking down bandwidth all over the theatre of operations. We had hundreds of T1 circuits available; but, of course, when the balloon went up and we went into full-time operations in the 100-hour war, those circuits were used to about 15 to 30 per cent of capacity. It was not adequate bandwidth for the need at hand; but we managed to get by with what we could make available. If you nail this stuff down in such a way that you cannot reuse it, then clearly you are going to run out of bandwidth very quickly. Let me try to ease that thought process a little bit: if you can reuse bandwidth then you do not need anywhere near as much spectrum or as much bandwidth as you might think you do. What do I mean by that? I am talking about virtually creating a high bandwidth sandwich between the fibre that is in the ground and these assets that are in orbit, and we do not have to invent anything new or violate the laws of physics to do this. There's a big

move afoot to interlink those objects in orbit with high-speed, high-capacity laser ‘pipes’. That part of the infrastructure is aimed primarily at bringing to the mobile user on the move the same capacity, the same power, the same speed that he has when he is plugged into the fibre in Garrison, such that he does not have to change his *modus operandi* when he moves out into the mobile venue.

So, step one: we are focusing on bringing greater capability by linking things together in orbit. Step two: bring agile, that is, laser beam linkage from orbiting systems to high altitude air-breathing platforms, like AWACS, like the joint STARS, like lots of other platforms, tankers, freighters—I don’t care what they are; as I said I classify these objects in a way unlike the way they have been looked at historically—in addition to their primary function, they can serve as high capacity gateways to the ground, air and sea forces and, perhaps later, can assume other operational functions as well. I do not want to outreach the technology, so I am telling you that we can do all this with technology that is available today. What is required is focus. What is required is an architectural framework to establish a common base line—the functional equivalent of a ‘building code’—that, while not defining the primary functions of the myriad objects and systems that make up an operational force, assures the correct *level of interoperability* among them all. It’s my view, based upon current discussions in the industrial community and among the military forces, that real progress is being made toward that objective. Those putting objects in orbit should be held to task in that regard; nothing should go up there without having the ability for laser cross-linking. At the high altitude, large platform level, there’s lots of carrying capacity, lots of power, lots of support mechanisms for accommodating the added capability for high volume packet passing, so why not drop that laser capability into them?

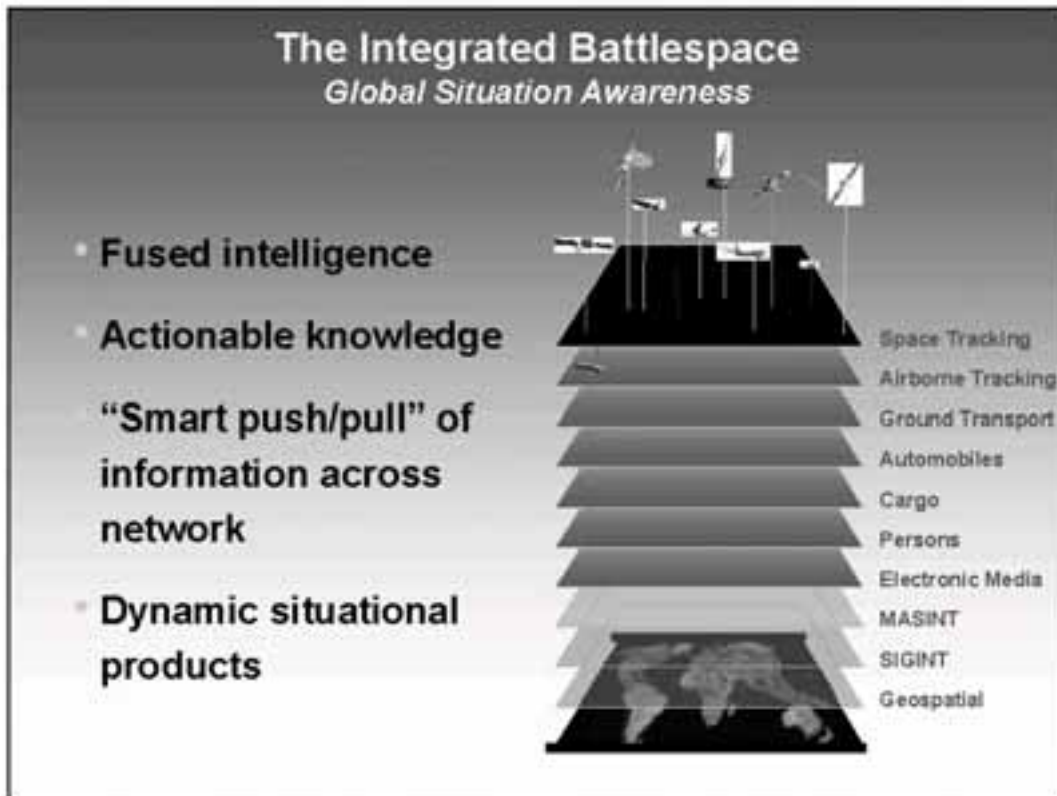
For that matter, why not drop it down even farther, subdivide it at that juncture and start thinking about the effects in the near future of cognitive radio technology. That’s called JTRS or FAB-T today—Joint Tactical Radio System, or Family of Advanced Beyond Line of Sight Terminals. Both are smart routers for high volume packet passing; both of are very effective in terms of emulating wave forms and allowing current systems to trade data—a very important factor in leveraging the new digital technology—but ultimately going digital means much more than that. Treated as elements of a system, every box on every platform can be assigned its own Internet Protocol (IP) address. Those boxes are all computers, albeit of varying levels of capacity, speed and operational capability, but whose functions—indeed, whose very designs—can increasingly be changed with a software download from almost anywhere, and are within the power of today’s networks. You can think of this as terabytes of data down to the high altitude platform level, gigabytes down to terra firma, and megabytes among the operative objects in the air, sea, and ground fight.



**Figure 6 – The Integrated Battlespace: Intelligence, Surveillance and Reconnaissance**

Figure 6 shows an array of objects of a different variety than the base communication types addressed earlier. This is the sort of array that, hopefully, will give us persistent surveillance of the operational space. There is nowhere near enough here to do that, but if they all can be linked together in the right fashion it is quite possible to integrate their respective capabilities to provide significantly greater visibility of the operational environment than can be expected today. Suppose all the sensors that are available in the operational platforms in the battlespace had IP addresses assigned: from the radar on an F/A-18, to the sensors on the Multi-Mission Maritime Aircraft, to various unmanned air vehicles and space platforms. Take the F/A-18, for example. I do not want to take that over from the operator, the guy that runs the machine, but if he happens to be situated in the right place and that sensor happens to be operative, if that radar is available to the operative network then intelligent software agents can access that data and make it a part of the options set for decision-makers in certain events. What we need is persistent surveillance. We do not necessarily need something in orbit hovering directly over the operational space. We need to take advantage of every single sensor source that is available to us in this environment—and there are hundreds, sometimes thousands of them. This boils down to accessing, fusing, and analysing that data and formulating useful intelligence products from all of the sensors that are operational in the battlespace. That is made possible by equipping each and every object that goes into that operational space with a certain fundamental capability; that is, the ability to communicate, to pass packets. It becomes an operational node in the communications and information handling environment. It drives, walks, crawls or flies into the operational space and as soon as it is within that venue it registers with the network. It tells the network what its

capabilities are, what its products are, what it needs from the network in terms of support—and it becomes integrated with that established network.



**Figure 7 – The Integrated Battlespace: Global Situation Awareness**

That gives us the potential, if we do this correctly, to create a multi-layered, fused capability to look at all the things on the right-hand side of Figure 7 and take advantage of that data—efficiently, virtually instantaneously, marshalling the resultant products into content suitable for the decision-maker, be he an individual soldier on the ground or the pilot of an aircraft, or a company, division or corps commander. You need what you need at the time that you need it, and so the system has to be constructed in such a way as to evaluate the requirement and seek products from relevant sources to meet the need. Embedded within the network will be the relevant commander’s intent and pertinent rules of engagement. The network will not forget such things. You and I have a tendency when we are getting shot at to find it challenging to remember rules of engagement—concentrating, perhaps, on ‘getting the hell out of there’. But the network is going to know what those rules of engagement are and, if they change, it will know what the changes were. So it will offer options in the decision sense that are consistent with intent and the rules of engagement and with the operative capabilities available in that network. There are myriad examples today of what, for the lack of a better term, I will call ‘islands of capability’ that employ examples of that sort of structure.

The missile defence system in formulation today is a global system. It is a good example of how to bring lots of things together that are already ‘rubber on the ramp’ today and cause them to interact in ways that they were not necessarily designed to do but from which new capability can be added to the environment—an example of the

‘force multiplication’ objectives of times past when the technology was perhaps not so well suited to achieve such effects. Take for example, the sensors aboard an *Aegis* Class cruiser—very good sensors, and when your objective is to find missiles in the early boost phase, determine their trajectory and ‘kill a bullet with a bullet’, then adding the capabilities of those *Aegis* ships to the ballistic missile defence network makes very good sense, even though that was not what the designers had in mind for such a system. So the command and control structures, the sensing structures and the response structures of the global missile defence programs are formulated such that we can leverage the capabilities of existing systems in concert with evolving ones to very good effect.

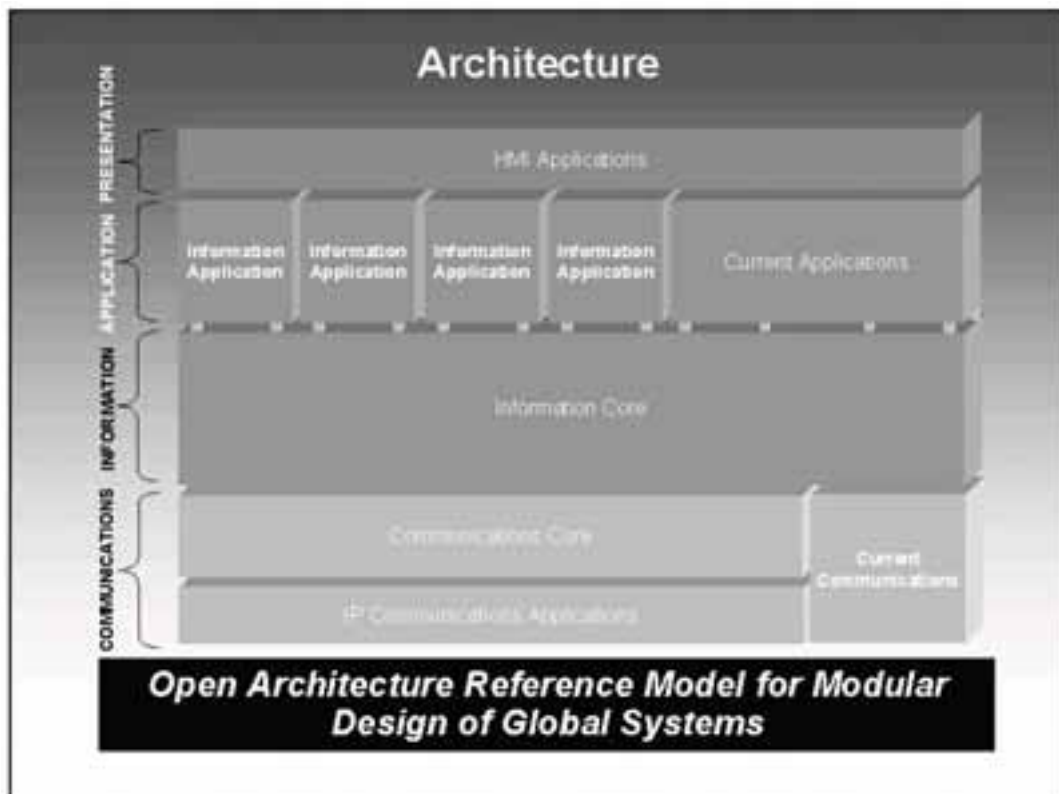


**Figure 8 – The Integrated Battlespace: Integrated Command and Control**

There are new programs that have come into being in just the last couple of years. The Future Combat Systems program you have heard referred to before is an entirely new way of acquiring technology. Historically, we have sought platforms that were better than existing platforms and expected that the infrastructure would be modified in some way to accommodate to the requirements of the new platforms, rather like putting the cart before the horse. Programs today are being formulated as systems requirements. The Future Combat Systems program is, first and foremost, a ‘system of systems’ design. The platforms that may be ultimately associated with this system of systems, while influenced by some essential attributes specified early in the program—for example, weight and size constraints and the need for common chassis among the platforms—will not be specified until the system requirements are known. In other words, the platforms will not be designed until the system design is complete and platforms will be designed consistent with the needs of the system. Now that is totally upside down from the way things have historically been done; but it is the way

that the Future Combat Systems program is put together. That is what we believe will happen in terms of the Navy’s FORCEnet, eventually, and the Air Force’s command and control (C2) constellation.

This brings us to the point where we need to think about the underlying substrate, the structure on which you build network centric capability. It is the only time I am going to use the ‘A’ word here. There is an architectural framework (Figure 9) that is necessary to accommodate to the ‘system of systems’ development structure.



**Figure 9 – Open Architecture Reference Model**

The lower two layers of the architecture framework shown at Figure 9 are absolutely essential to achievement of the concepts outlined here. An integrated ‘substrate’, composed of a core information handling and services layer, integrated with a communications core based on standards appropriate to complex systems of systems design and production, is the basis of network centric operations. The Internet Protocol (IP) is the foundation standard. Internet Protocol Version 6 will provide the advances needed in terms of increased address space, security, and mobile network support needed to leverage new and evolving technology. The architecture framework we are addressing in this regard must be completely non-proprietary, employ open standards and encourage industry to inject common ‘DNA-like’ properties into its products—I will talk more about that in a moment because that relationship is one that is incredibly important—but it is an open architecture reference model to which modular systems can be designed. If you look at the upper layers of Figure 9, and this is as much detail as I am going to go into, the capability layers, the information applications and human-machine interfaces in general have to be consistent and compliant with the lower layers of this architecture reference model. We need to

populate this with enough flexible products and capabilities that the designer has a range of options available so that he can do cost and capability trade-offs. Not everything requires zero-latency, maximum quality of service. If you are into fire support where you need that, fine, you have to pay the price for bringing in that kind of capability, but if some latency in the decision processes to be employed is tolerable, then a wider range of capabilities can permit addressing the requirements at lower cost. What we are after is as much commercial off-the-shelf technology in the products that go into those lower two layers as we can employ. What does this do to the competitive environment in terms of addressing new ‘systems of systems’ requirements? It allows those of us who are in the systems integration business to leave those lower two layers to the domain of off-the-shelf products and move valuable engineering resources up to where it really counts, where we get the best return on our investment and where the customer gets the best return on his investment—that is, new capabilities, the ability to address the requirements at hand and not have to worry about reinventing those lower two layers for every new program that comes along. Now that is a methodology that requires both the customer requirements to be properly codified and industry to engage at the right level to satisfy the need.

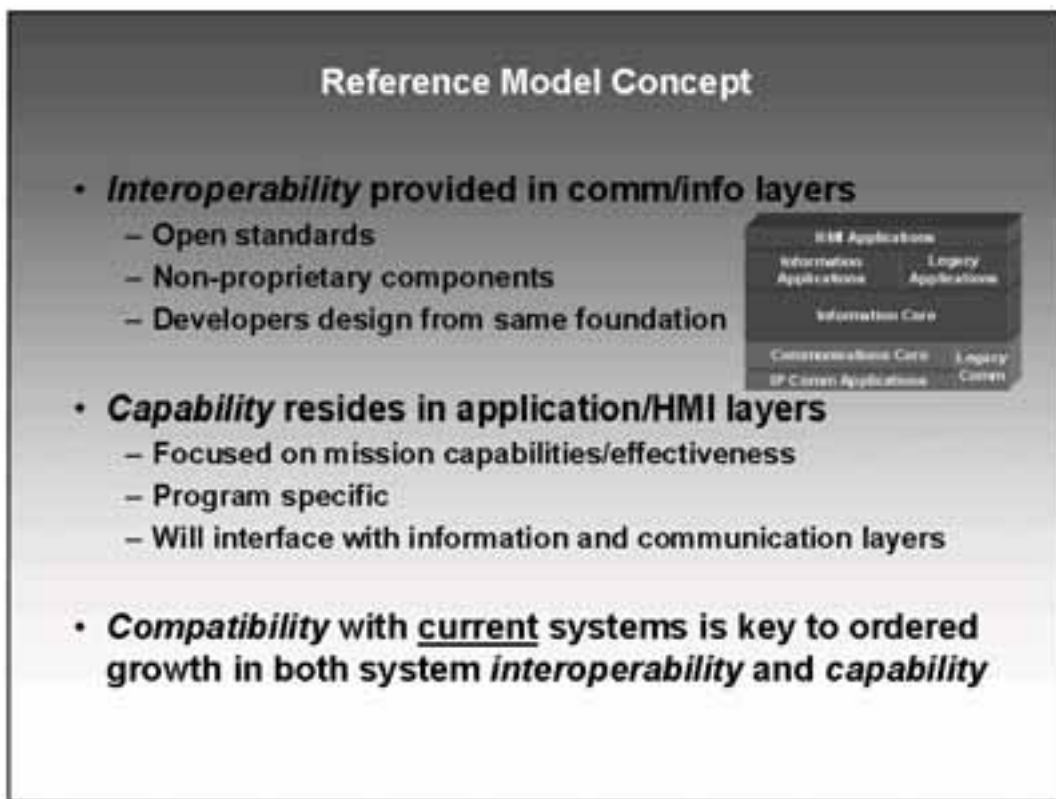


Figure 10 – Reference Model Concept

Interoperability requires open standards at those two lower layers. It requires non-proprietary components and it requires that developers design from the same foundation. How in the world do you get all of industry to cotton on to that idea? Let me talk about that more in just a moment. System capability resides in those upper layers as I have alluded to and that is where we all get the biggest ‘bang for the buck’ on our investments. Compatibility with current systems is paramount to this and, while we need not drag everything in the operational space to the level of capability

that future systems will bring, we can bridge current systems to future ones with cognitive radio technology; that is, through the application of JTRS and its like, to allow these things to share data. That, after all, is the minimum level of interoperability necessary to be effective in today's world. Beyond that, when we design future systems we will design in the same way that the Future Combat Systems program has been put together; develop system requirements first and then design platforms and subsystems consistent with those requirements.



Figure 11 – Integrated Battlespace Objectives

Figure 11 summarises in very broad terms our objectives for the integrated battlespace. We really have to institute at least a minimum level of interoperability as an inherent property in everything that we build and everything that is available to us in current systems. That is not as difficult as it might sound. Not every functional capability in current systems is equally valuable to us; therefore, we can take this on a case by case basis and address it in a current systems sense. We need to demonstrate network centric operations and its advantages. You have to be able to show people what leverage they get from bringing everything together in a network sense. We have to be able to leverage the synergies associated with the government's capabilities and its derivation of requirements, and industry's pushing and developing of technology. Making sure that those things come together correctly requires a different relationship between government and industry than that to which we are historically accustomed; you have heard others allude to that. We think we have an approach to this that is beginning to get traction. Then, finally, we must keep pace with technology. We would really like to be able to design things and execute programs such that current technology can be brought to bear on operational requirements while the technology is still current. Current acquisition processes, if followed on historical terms, can

mean the technology turns many, many times within the length of a program. That virtually guarantees obsolete capability, based on the current state of technology, when something that has taken five or ten years to develop is finally delivered; you have heard others say, ‘You ain’t gonna like it all that much any more!’. I personally believe that the velocity for improving that trite process is going to come through industry collaboration. How can this be made to happen? Well, Figure 12 summarises a significant fraction of industry views on this.



**Figure 12 – Industry as a Partner in Transformation**

There is no doubt in the minds of most producers and users of information technology as to who the owner of the requirements is, and there is no doubt about the need for defining a defining process for operational requirements. However, we believe that there is room for collaboration in that process. It would be very helpful if industry were there with some sense of where information age technology is headed and what the art of the possible is. You have heard references to spiral development many times. The idea would be for industry and user to ascertain collaboratively a reasonable 80 per cent solution and begin with that—most of it can be handled within current technology. The other 20 per cent of the requirement is probably going to change as the system evolves and as the technology advances, and can be more appropriately addressed later. That approach helps evolve the operational architecture, or your enterprise level architecture, which is both a process in work and a vision to help industry better understand your needs. Industry, on the other hand, has a responsibility to evolve the technical architecture and the basic infrastructure to accommodate the increasing demand for global ad hoc self-organising networks, with help from its customers.

Industry, however, has not stood up to this responsibility until fairly recently and I will talk about why I believe that in a moment. Industry has the ability to implement, integrate and complement operator requirements at a rate that is consistent with the development of the technology today. It can leverage technology in ways the customer cannot because, no matter what you say about your requirements being very important (and no one denies that), your requirements are no longer the driver in the advancement of technology. The requirements driving technology today are consumer and marketplace demands, not military requirements; but, having said that, we can leverage consumer demand on your behalf to provide huge advantage for military operations.

In fact, fostering a common understanding about modular systems and the need for network centric operations and effects-based operations can be aided and abetted immensely by the right relationship with industry. Promoting that multiplier effect also will provide value to numerous other activities and domains. That may not be too obvious as we begin this journey by enabling current systems to exchange data more effectively, but you are going to see a capability bump almost immediately as that seemingly commonplace effort begins to take effect, and when we get to the point where the design of new systems consistent with this fast evolving technology starts to produce real capability you are going to see power law improvements in agility, speed, and the ability to address asymmetric requirements. This has the added advantage of advancing a healthy competitive space to give you the best prices and the best capabilities in the shortest time and it will open up for industry new market opportunities and, in fact, entirely new markets.

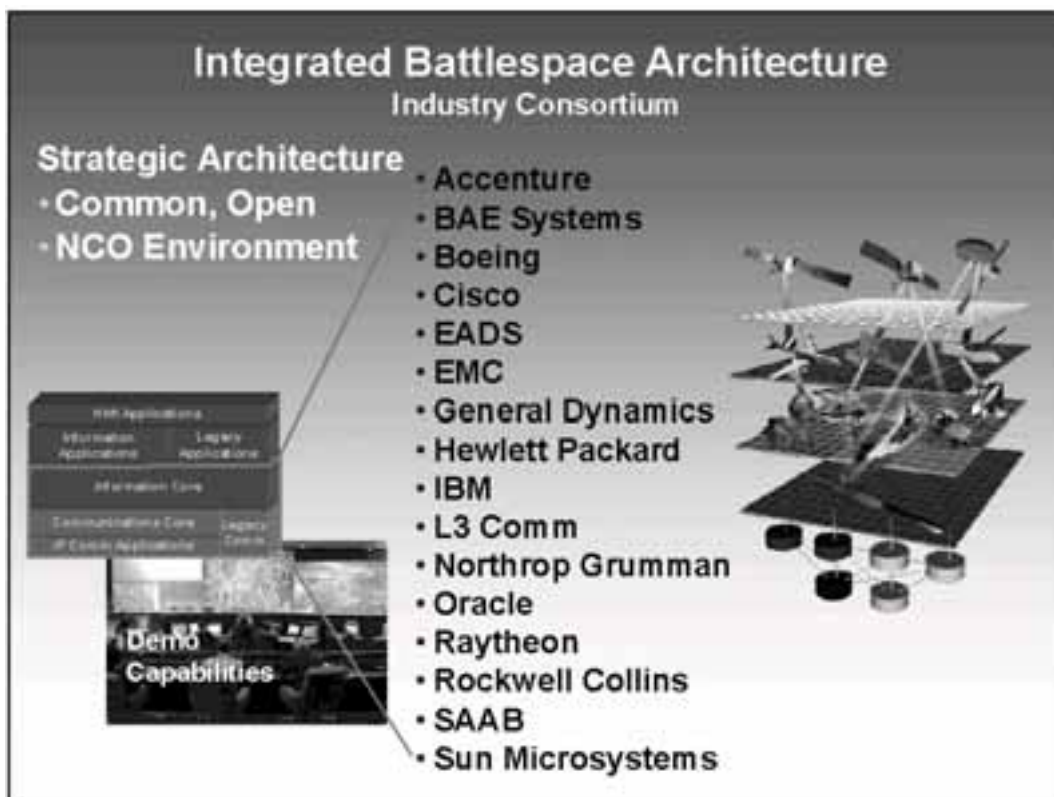


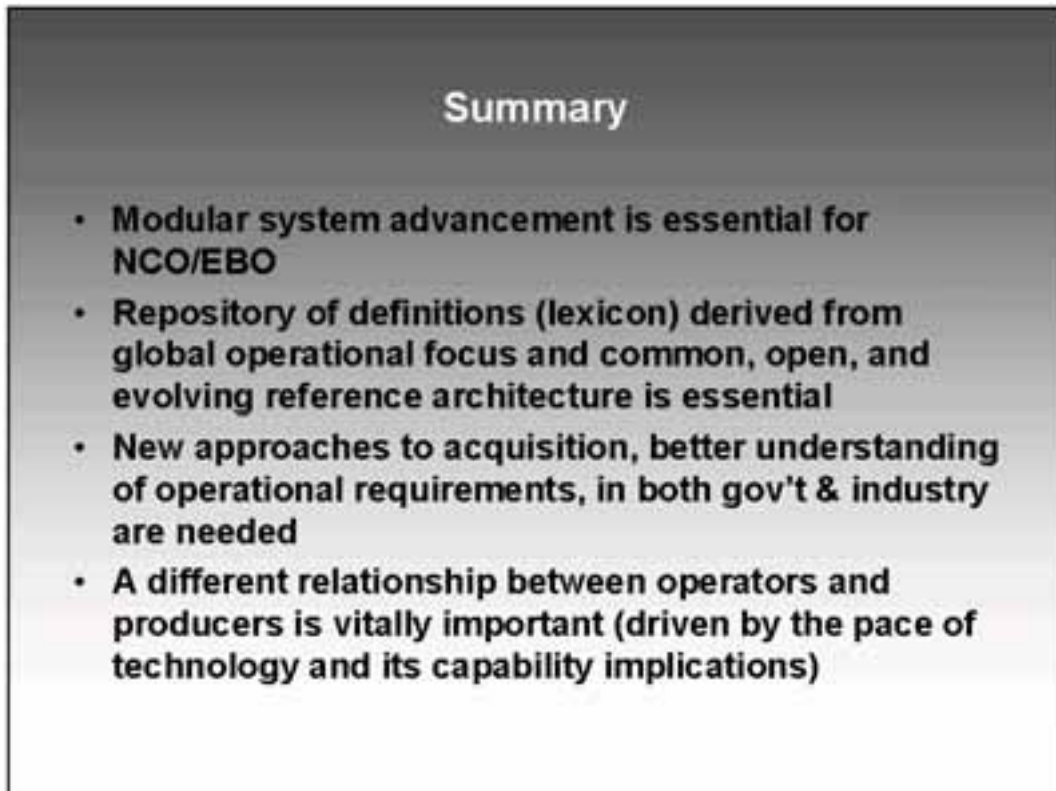
Figure 13 – Integrated Battlespace Architecture: Industry Consortium

Now let me address the basis of that claim. A year ago a dialogue began among the 16 companies listed in Figure 13 to test the premise that it was possible to create an industry consortium that would agree to the principles that I have just tried to describe. The lower two layers of that architecture reference model I described earlier (Figure 9) are the venue of these 16 companies going into this. They began meeting to determine the following:

- Is it possible to do this?
- Is there a value proposition in doing this?
- Do we want to do this?
- Does it make sense for us and, hopefully, a larger collection of companies?

Interestingly enough, the first couple of meetings were just really ugly. Nobody trusted anybody. We found out right away just how valuable information is because everybody hugged their information very closely and let out just a few molecules here and there. It was a very interesting sort of a proposition. We put on the table a couple of ‘straw man’ principles associated with this as initial propositions—a vision statement and a proposed organisational approach. After several meetings it became apparent as the teams we created to analyse this—a technical team and a business team—that the concept was starting to get traction among those 16 companies. In June of this year we decided to incorporate a new not-for-profit corporation called the Network Centric Operations Industry Consortium (NCOIC). These 16 companies were the charter members of that consortium. Since then, the population has grown to 27 companies and we are going to announce at the end of this month at the National Press Club in Washington DC the formation, objectives and deliverables of this new industry enterprise.

I hope you realise that this has immense implications for you because those who joined the consortium have agreed that if they want to bring anything proprietary into the architectural framework that I have just described, that proprietary element instantaneously becomes public property. Proprietary is not allowed. Open systems are what this is all about. We have all agreed that it does not make any sense for us any more to allow program after program to come into place where we must re-invent those lower two layers of that structure, with the subsequent guarantee that what’s being produced will not be interoperable with anything else. Instead, we are going to implant in everything that we produce the same fundamental ‘DNA’ that brings with it the latent capability for the product to become a node in the emergent global environment. Now I think you will agree that is a huge step forward. The outcomes to date of the Network Centric Operations Industry Consortium are summarised in Figure 14.



**Figure 14 – Summary of Outcomes of Network Centric Operations Industry Consortium**

It has really taken us about three years to get this consortium going because it took me a year and a half or more just to get these guys to agree to a meeting—thus this is not a trivial proposition. But I am absolutely convinced on the basis of hard experience that the modular system approach is the only way to bring the power of information technology to bear on your operational needs while it is still current. It gives us the ability to produce more things faster, in developmental spirals, and to continue to evolve new capabilities faster, at lower cost, and in fully interoperable context. Industry has agreed, through this consortium, to take ownership of that architecture reference model and continue its evolution it, move it along, consistent with where the technology goes. We intend to use existing standards that you demand and that are useful to you; but remember that standards atrophy just as quickly as any other element of technology, so we need to continue to adopt new standards and bring those to bear as they emerge. Industry can do that better than anyone else. A repository of common definitions, a global information technology lexicon is in the works of the consortium. We need a lexicon that says the same thing to everybody—when somebody says ‘architecture’ and when somebody says ‘network centric’ or ‘net centric operations’, or whatever the term might be, that is going to be a definition in the NCOIC lexicon. You are going to see new approaches to acquisition as a consequence of this. It has international implications. You can see that there are international companies involved in this. There will be many more. There is a different relationship developing between industry and government in the United States, in Europe, and other continents where other companies are represented.

I think I will stop there and try to answer any questions you might have.

\*\*\*\*\*

## ***DISCUSSION***

*Major Dave Schlosser (USAF):* I noticed on your list of consortium companies that one big name was missing and that was Microsoft. With our F-16 we had some problems with drivers in the new Microsoft systems with our test equipment. How is Microsoft going to be engaged in your new consortium?

*Lieutenant General O'Berry:* That list that I showed was deliberately limited. We wanted to get 15 or 16 companies that were representative of all the elements of industry that were appropriate here. If we had invited everybody in at the beginning it would have been very difficult to formulate a strategy and an organisational structure, so our objective was to keep it sort of exclusive for the formative stage of all this. I will tell you now that Microsoft is a member of that consortium. Lockheed Martin was missing from that list; it is now in that consortium. Thales also has joined. There are a number of others who have joined since we opened up the membership to everybody on 27 June [2004] and there will be many more. This enterprise has got such traction now that people feel obliged to join, if for no other reason than to find out what the heck it is all about. So they are there and I am convinced that they will all contribute significantly.

*Flight Lieutenant Fiona Peacock (RAAF – No 28 Squadron):* Sir, thank you for your vision of these technological potentials and particularly your industry consortium—I think that is a significant step. I found that your paper was an interesting contrast to the two earlier ones this morning, which provided us with the historical and security contexts that we are now operating in. I really acknowledge the importance of future scenario work and emerging technology. Something that I am particularly concerned about is the current threat to Australia's national interests and, obviously, it impacts equally on the US—the very real threat to Australian and American military and civilian lives. And as we all know, this current threat is an asymmetric one and we are not facing conventional, state-based warfare. We are faced with terrorism, extremist ideologies, suicide bombers and vehicle bombs. How can the RAAF adapt to this current threat and apply NCW against an adversary that doesn't get detected by satellite imagery or IMINT?

*Lieutenant General O'Berry:* That's an excellent question. Let me preface my response to that in the following way. I blasted through a tremendous amount of terrain here in just a few minutes, so I apologise up-front for not having the ability in that short time to address all the security concerns and the response concerns for a lot of things non-military in that context. The best way I can answer you, I think, is to use the model that seems to be emerging right now in the United States in terms of homeland security and how you deal with this increasingly asymmetric kind of threat. I will offer the following. We found that the more that you network things together, the more capability that you have to respond effectively, the greater the improvement in global situational awareness, bringing modern decision-support tools to bear on the issues and creating responses very quickly. We can demonstrate that in real systems and real hardware and software in facilities like the Boeing Integration Center, which

is really quite stunning when you look at how long it takes today in very complex situations to build complex kill chains. I mean, employing this new methodology it takes only milliseconds to create options for addressing a particular event. If the commander or the decision-maker does not like any of those options, he or she can say, 'None of these are adequate for this situation. Readdress it. Fix it.' And the network will respond within seconds, ruling out assumptions that were tested in the first set and produce a completely new second set of viable options. The issue here is speed of decision, the ability to bring as much information as is available in the operational space to bear on the decision set and the options set, and do it very, very quickly. So, yes, we are faced with asymmetric requirements and that condition is going to expand and become more complex. We know that the bad guys, for fairly low levels of investment, can go to Radio Shack or some place else and buy bits and pieces of this kind of capability and cause difficulty for us, to say the least. But the focus that brings all of this together in different venues will allow us to integrate the capabilities of everything relevant in the network on demand and produce unprecedented situational awareness and good decision support tools for the warrior. Networking things together and providing option sets very quickly, asymmetrically if you will, is just as important to homeland security people, to the medical field, to any venue of human endeavour that I can think of, to varying degrees. So it is not going to solve the problems instantaneously but it is a means of bringing new technology to bear on current issues much more quickly than any other way that we can think of. It requires focus; there is no new technology required to make this happen.



# NETWORK CENTRIC WARFARE DOCTRINAL ISSUES<sup>1</sup>

GROUP CAPTAIN CHRIS FINN, RAF

In a conference that examines the future use of air power in the context of the developing technologies and concepts for network centric warfare, it is not surprising that a lot of the papers already presented have concentrated on those technologies and on the promise of Network Centric Warfare (NCW) in a 15–20 year timeframe. The intention of this paper is therefore to take a slightly different look, that of the near to medium-term of five to ten years, from the perspective of the doctrine writer and also to examine NCW to see how it fits with other emerging doctrinal themes.

The scope of the paper is, therefore:

- to identify the role of air power doctrine,
- to look at the historical development of air power doctrine and the emergence of key concepts,
- to analyse the interaction and implementation of those key concepts, and finally
- to draw some conclusions.

The overarching doctrinal statements for the USAF, RAAF and RAF are laid down in *Air Force Basic Doctrine*, *Fundamentals of Australian Aerospace Power* and *British Air Power Doctrine* respectively, but what is the purpose of these books and the doctrine contained within them? At one end of the scale there are tactics, techniques and procedures (TTP) for specific equipments and environments but the doctrine contained in these documents is much broader than that and sits at the strategic and operational levels of war. Perhaps the best explanation of this doctrine was made by USAF General Curtis E. LeMay in 1968 when he said:

At the very heart of warfare lies doctrine. It represents the central beliefs for waging war in order to achieve victory. Doctrine is of the mind... **It is fundamental to sound judgement.**

There are also a number of common characteristics between the doctrines laid down in these manuals. The first is that they are a statement of fundamental principles and are thus enduring, which in itself can be seen as a test of the validity of emerging doctrine and thus highly relevant in an examination of NCW. They also all address the ‘what’ and ‘why’ of doctrine rather than the ‘how’, which is the business of TTP, and are applicable here and now or in the relatively immediate future. Thus a second test can be applied to emerging doctrine, that of relevance within a five to ten year timeframe. In the context of an earlier paper, the doctrine should address the ‘initial’

---

<sup>1</sup> This paper is subject to Crown copyright protection.

and the ‘early transitional’ periods of the implementation of NCW. It would also seem, not least from the other papers presented at this conference, that air power doctrine is technologically led, reflecting the art of the possible. Airmen are intrinsically happy with this. Two other aspects of doctrine emerge, in how it is used: the first being to explain the ‘what’ and ‘why’ of air power; and the second to engender in people a desire to seek greater understanding. Air power doctrine is really a statement of philosophy and principles, and thus a human, intellectual issue which is evident in the following brief overview of the development of air power doctrine.

By 1 July 1916, the first day of the Somme offensive, all the ‘core capabilities’ of air power were evident or had been identified. Air mobility was limited and air-to-air refuelling had not yet been invented, and close air support was very rudimentary. However, in addition to achieving control of the air to enable other air and land operations, a major role of the Royal Flying Corps (RFC) at this stage was controlling artillery fire. The weight of radios and batteries at the time were such that only transmitters were carried and aircraft and thus, in modern parlance the pilot, or the observer of a two-seat aircraft, fulfilled the role of both the sensor and the decision-maker, passing their orders to the shooters, the artillery. Feedback in this case was almost instantaneous, they observed the fall of shot and corrected for it. Interestingly, the use of clock codes and ranges from a known point as a method of correcting artillery fire was developed in parallel on both the Western Front and in the Middle East but because no overarching doctrinal organisation existed it was not communicated between theatres. By 1918, the RAF had formed the ‘Independent Force’ latterly under the leadership of Major General Trenchard, who developed strong views on the independent use of air power to achieve strategic effect. However, the technology in terms of size of bombs and accuracy of delivery, and methodology in terms of analysing which targets to attack greatly limited its application. Shortly after the war, the RAF produced its first doctrinal document, *CD22*, which was shortly replaced by the first edition *API300 – Air Operations*, which very much reflected the views of the time of the primacy, and indeed the inviolability, of the strategic bomber. At the same time, officers of the US Army Air Corps’ Tactical School at Maxwell Air Force Base in Alabama were developing the strategic bomber theories that would lead to the ‘industrial web theory’, which would form the basis of the US plan for the combined bomber offensive against Germany in the forthcoming World War. But fortunately there were other thinkers who were not so wedded to the bomber doctrine. The then Wing Commander, later to be Marshal of the Royal Air Force, Sir John Slessor in his seminal book *Air Power and Armies* made clear the requirement to achieve both control of the air and to fight an integrated air/land battle. Technologically the RAF was moving, albeit slowly, from the biplanes of the inter-war years to monoplane bombers, such as the Fairey Battle and the twin-engined Blenheim, and the specifications for the four-engined bombers, starting with the Stirling, laid down before World War II started. On the air defence side, initially as an Air Commodore but later to be Commander-in-Chief (CINC) Fighter Command as an Air Chief Marshal, Sir Hugh Dowding fulfilled a number of procurement roles, the most important of which was to be Air Member for Supply and Research from the mid-1930s. Dowding’s system, the integration of hostile tracks generated by the Chain Home radar system and by the Royal Observer Corps in the filter room at Fighter Command Headquarters at Bentley Priory, with the recognised air picture then being passed to the Group operations rooms, such as 11 Group at Uxbridge, and then to the Sector airfields and to the fighter squadrons, was the world’s first Integrated Air

Defence System (IADS). It was also a good example of what we now come to recognise as the principles of NCW, with the sensors, decision-makers and shooters being clearly identified, and information and decisions being handled so as to maximise the effectiveness of the system as a whole. An amendment was issued to *AP1300* in 1939 which effectively said that the document was out of date and a further amendment would follow shortly; and then a subsequent amendment in 1940 significantly updated air defence and strategic bomber doctrine in particular.

In terms of bomber doctrine, both the CINC of Bomber Command, Air Chief Marshal Sir Arthur Harris, and Commander of the 8th Air Force, General Spatz, shared the same view about the ability of air power to achieve independent strategic effect through the medium of the strategic bomber. Where they differed was in how this was to be achieved through attacking industries and oil respectively, but the arguments were driven by the technologies of the time and the differing policies with respect of daylight and night-time bombing. The ‘Point Blank Directive’ of 10 June 1943 was entirely effects-based in that its initial primary object was to seek the destruction of enemy fighters in the air and on the ground in order to achieve Allied air superiority by the time of the Normandy invasion. Effects-based arguments emerged again in the run-up to D-Day, particularly as articulated by the Deputy Supreme Allied Commander, Air Chief Marshal Sir Arthur Tedder, and his Scientific Adviser, Lord Zuckerman, which involved both tactical and strategic bombers being used in the ‘Transportation Plan’ both to isolate the Normandy battlefield and to contribute to the strategic deception plan (Operation *Fortitude*). Having won the argument about attacking transportation systems, which directly isolated the battlefield, rather than oil production and storage, which would do that through the secondary effect of decreasing German land and air power mobility, further debate emerged about the relative merits of attacking bridges or marshalling yards. However, the underlying logic was that of the effects-based approach as we would describe it today. The *AP1300 – Operations* of the inter-war years, which was issued in 1957, amended in 1964 and then allowed to wither on the vine in the 1970s, again emphasised the primacy of the strategic bomber, but this time nuclear rather than conventionally armed. The RAF at this stage collectively stopped thinking about the operational level of war, retreating into a Central Front, citadel mentality, where the effort was now on producing and constantly updating the complex NATO operational plans for all possible tactical options to counter a Soviet attack on NATO.

The Falklands War of 1982 was something of a wake-up call for the UK defence establishment in that it started people thinking about how to exercise command and control in expeditionary operations and highlighted the essential nature of air-to-air refuelling (AAR) in those operations. It must also be remembered that, unlike the USAF and the RAAF, the RAF did not experience first hand the Vietnam War. However, one outcome of the Vietnam War which did affect us, although we were not to realise it until 1990/91, was the creation of Exercise *Red Flag* in which regular RAF participation started in 1977 and continues today.

The fall of the Berlin Wall and the invasion some months later in August 1990 of Kuwait by Iraq marked the sudden end of the NATO certainties of the central region for the RAF. The air campaign plan, codenamed Operation *Instant Thunder*, which had been put together in September 1990 by the ‘Checkmate’ team under Colonel John Warden USAF, postulated the use of air power alone against targets which,

when neutralised, would lead to strategic paralysis of the Iraqi regime. The underlying philosophy would have been clearly recognisable by both Harris and Spatz, and marked the start of the contemporary use of 'effects-based' methodologies. *Instant Thunder* was, of course, not implemented in isolation and the *Desert Storm* air campaign had equally as much of the tactics of the central region of NATO that had increasingly been played out over the Nevada Desert as more and more NATO nations participated in Exercise *Red Flag*. It was here that the hidden benefit of *Red Flag* became obvious to the RAF when after 14 years of participating in the Exercise, British crews and headquarters personnel were able to integrate almost seamlessly with their American colleagues.

The operations in the Balkans in 1995, Kosovo in 1999 and Sierra Leone in 2000 had little impact on RAF doctrinal thinking, were not networked in any great sense and, particularly in the first phase of the Kosovo campaign, had no effects-based underpinning. In Operation *Enduring Freedom* in Afghanistan in 2001 the RAF did not provide any offensive air power, although all the other roles were well represented. Although a relatively small campaign in terms of sorties flown, as Dr Alan Stephens has pointed out in an earlier paper, there was some novel networking, particularly in the case of forward air controllers operating not in support of regular land forces but instead supported by irregular ones.

It has been suggested that Operation *Iraqi Freedom* in 2003 was planned and fought using an effects-based methodology supported by an emerging net centric capability. At the operational level the campaign had all the hallmarks of an effects-based plan (this is discussed later in the paper) but its implementation much less so. If we can consider NCW as simplistically the linkage between sensor, decision-maker and shooter, although it involved many work-arounds, the Coalition was able to join together numerous disparate systems, such as the Blue Force Tracker, which provided GPS-based position data, and tanks, armoured fighting vehicles (AFVs) and guns etc, to a common database to provide a common operating picture at Corps level and above. While targeting data was passed to aircraft by a mixture of data links and voice, there was no facility to pass aircraft a parallel and automated plot of friendly positions. However, the key failure in the system was that of Battle Damage Assessment (BDA), which firstly was not timely enough to keep up with the tempo of operations and was conducted in a purely kinetic sense (ie. what had been destroyed rather than what effect that destruction achieved). So what doctrinal points can be made from this very quick overview of 90 years of the use of air power?

Firstly, it would appear that the core roles of air power—which for the RAF are: control of the air, air operations for strategic effect, ISTAR, rapid global reach, and joint force operations—are still valid in describing the operational level 'ways' available to an Air Component Commander and hence the effects he can seek to achieve. Secondly, the change over the last 13 years in the use of precision weapons, from seven per cent overall in Operation *Desert Storm* to 68 per cent in Operation *Iraqi Freedom*, is such that the ability of modern air forces to deliver lethal force to a designated point in time and space is now assumed. Thirdly, the concept of 'effects' is almost as old as air power itself and is now mature. Fourthly, NCW, which is again by no means a new concept, is now technologically viable and the problems are as much as how to get the most out of legacy systems as how to procure and field new ones. Finally, technology provides a legitimate asymmetric advantage to Western armed

forces that, in its turn, drives opponents to seek their own asymmetric advantages which are neither technological nor legal and aim to play to the weaknesses of those who come to rely more and more on technology.

Three factors have therefore emerged: one physical, precision weapons; one conceptual, that of effects; and one an amalgam, that of NCW. None are wholly new but their relationships now need re-examining because, as Professor Babbage points out in an earlier paper, NCW cannot be viewed in isolation.

The first relationship, particularly when one compares recent conflicts with, say, World War II, is that precision weapons have enabled the adoption of an effects-based approach. However, that begs the question what is really meant by the term ‘effects’? The first viewpoint is that an effects-based approach is simply a formal recognition of the Clausewitzian linkage between policy aims and military force. This has been developed in the UK into the ‘strategy to task’ methodology in which a series of linkages has been created from strategic level end-state through a series of operational and tactical objectives down to each specific military act. This has particular utility in establishing the relevance, and hence the legality, of any individual military act to the military advantages to be gained at the operational and strategic level, and thus drives a very centralised and top down targeting process. The next two viewpoints are often, but not necessarily, linked, which are that effects-based approaches work only at the strategic level and that they are purely coercive in nature. A further extension of these theories is that coercion can be achieved by perception management rather than by military force. Another viewpoint is that of the systems approach, which views all actors and the events they cause as being inter-dependently linked, as is evident in this RAND definition:

Effects-based operations are operations conceived and planned in a systems framework that considers the full range of direct, indirect, and cascading effects, which may—with different degrees of probability—be achieved by the application of military, diplomatic, psychological, and economic instruments.<sup>2</sup>

The last viewpoint takes that on a stage further, to view all activities, be they at the strategic, operational or tactical levels, to be part of an infinitely complex system where the permutations of actions, reactions and interactions can only be solved by computer-based ‘knowledge systems’. Taking all these different viewpoints, there seem to be three fairly common facets of an effects-based approach, one or more of which occur in the different models outlined above. These are:

- An effects-based approach concentrates on the outcomes to be achieved as opposed to the mechanisms used to achieve them.
- The effects-based approach is applicable at all levels of war. Any mechanism appropriate to the particular level may be considered. There should be a coherency between the desired outcomes at each level.
- Effects may be direct or indirect, planned or unplanned, positive or negative; their interactions create subsequent and cascading effects.

---

<sup>2</sup> Paul K. Davis, *Effects-Based Operations: A Grand Challenge for the Analytical Community*, RAND, Santa Monica CA, 2001, p. 7.

The first bullet-point above is not new but needs constant restating. The second argues that if the methodology works at one level of war then it is equally applicable at all of them and that the linkage between them is that known as ‘strategy to task’. The last bullet-point highlights the problems with an effects-based approach, which is why some commentators perhaps suggest that it should only apply at the strategic level, because as one goes to the operational and then the tactical level the number of permutations of actions and reactions become impossible to handle.

In terms of the emergence of the three doctrinal elements of networks, precision and effects, one of the key thrusts of this conference is how networks enable the use of precision to achieve their desired effects. The UK approach to net centric warfare—or, as we term it, network enabled capability—has already been covered in Air Vice-Marshal McNicoll’s paper, but in the context of this paper the most useful definition is:

NEC is crucial to the delivery of military **effect**. ... NEC will improve communication and understanding of the strategic and military **intent** throughout the chain of command. Through NEC the command structure will improve its responsiveness to events on the ground and have the flexibility to respond in near or real-time to fleeting targets, even where **higher-level decision-making** is required prior to engagement.<sup>3</sup>

While this paper will shortly return to the issues of command, intent and high level decision-making, we need to examine the interplay between the concept of effects itself and the emerging networks. Many nations, the UK included, specifically link the synergy of conducting a network and effects-based campaign, but there is no reason why an effects-based campaign should be networked (Operation *Instant Thunder* was not) nor why an entirely attritional-based campaign could not be efficiently conducted through the use of networks. It appears, therefore, that in all the literature about network enabled capability, two major tenets of air power—that we centralise its command and control and decentralise its execution and practice mission command—are now becoming the ‘mantras’ of NEC. However, do we really understand what they mean, particularly as they are becoming the key to how net centric warfare is conducted? The following is the current *AP3000* definition of centralised command and decentralised execution:

Centralized control promotes an integrated joint and multinational effort and enables air power to be employed to meet the priorities of the JTFC.

No single commander can direct personally all of the detailed actions of a large number of air units or individuals. Therefore, decentralized execution is essential to mission success. It is accomplished by delegating appropriate authority to execute tasks and missions. Decentralized execution allows subordinate commanders to exercise mission command.<sup>4</sup>

Whilst the reasons for centralised command are well known and can perhaps be best expressed as the need to prevent the frittering away of air power into ‘penny packets’, those reasons for decentralised execution are not well known and the meaning,

---

<sup>3</sup> Secretary of State for Defence, *Delivering Security in a Changing World*, Defence White Paper, Ministry of Defence (UK), December 2003.

<sup>4</sup> *AP3000 – British Air Power Doctrine*, Third Edition, Directorate of Air Staff, Ministry of Defence, 1999, p. 1.3.6.

context and application has regularly changed. In the NATO central region during the Cold War, the highest headquarters was AIRCENT. Below this the two Allied Tactical Air Forces, 2 and 4 ATAF, commanded the air assets on a geographical basis. Below the ATAFs, the Allied Tactical Operations Centres (ATOCs), of which there were four or five to each ATAF, tasked individual missions on the basis of primary airfields being allocated to each ATOC. The reasons for this were simple. In the days before universal IT, each individual mission was tasked on its own Air Task Message (ATM), which was handwritten or typed by the staff officer in the ATOC. Complex missions, such as ‘Option Alpha’ against Warsaw Pact main operating bases, were pre-planned to enable rapid execution. Furthermore, the ATOCs provided redundancy in case of communications failure or enemy attack, thus command was centralised at the ATAFs who issued the daily Air Operations Directives (AODs) and execution was decentralised to the ATOCs. By the time of *Desert Storm*, the procedures, at least for the USAF, had changed and the multiple ATMs were replaced by a single Air Tasking Order (ATO), which with the Special Instructions (Spins) and the Airspace Control Order (ACO) provided all the details necessary for flying all missions, both pre-planned and on call, in a 24-hour period. In fact, for those who had previously attended Exercise *Red Flag*, the ATO was no more than the ‘frag’, the daily *Red Flag* flying program, writ large. One element of the air headquarters generated the master attack plan for the day, the equivalent of an AOD, and another element produced the ATO, which was then executed by the current operations cell. Thus, there was still delegation but it was now within a single headquarters. While there had been discussion about adopting what was in effect a central region model by forming a second Combined Air Operations Centre, or CAOC, in Turkey, this was not deemed necessary and with only the fairly rudimentary computer support available at that time, the Coalition Air Headquarters executed an average of 1000 offensive sorties plus supporting sorties in every 24-hour period for 44 days.

Operations *Deliberate Force* and *Allied Force*, in the Balkans in 1995 and 1999 respectively, were examples of centralised control and centralised execution where, because of the scale of campaign and the limited number of offensive sorties per day, in both cases the USAF’s COMAIRSOUTH in the CAOC at Vicenza was able to direct both the planning and execution of each day’s ATO, sometimes in a very hands-on fashion. Operation *Enduring Freedom* in Afghanistan was the smallest post-Cold War conflict in terms of sorties per day, an average of 83 per day over 78 days, and here the tactical air headquarters was in Saudi Arabia, 1140 nautical miles from Kabul, and the operational headquarters, CENTCOM, in Tampa, Florida, a further 5880 nautical miles from Prince Sultan Air Base. Finally, for the recent Operation *Iraqi Freedom*, where there were around 1000 offensive sorties and 1000 supporting sorties per day for a 21 day period of intensive combat, the *Desert Storm* model of centralised control and decentralised execution within the same headquarters was again followed. Simplifying the terminology one could suggest that: centralised = concentrated; decentralised = distributed; command = authority; control = management; and execution = action. To that end, centralised command and control and decentralised executions are just statements of the blindingly obvious. It is only by looking at the last sentence of the *AP3000* definition quoted above, ‘Decentralized execution allows subordinate commanders to exercise mission command’, can one see that the real issue is in fact how command is delegated and not particularly who does what.

Mission command, then, is the key. Most people are familiar with the way it is implemented in that subordinates are given the commander's intent, that is the reason their actions must support. They are told the effects to achieve and why, they are resourced and they are allowed to conduct their operations with the minimum of control and the maximum of freedom. However, what are less often talked about are the constraints on mission command, which are: physical, spatial and temporal; resources; rules of engagement; and targeting policy. NCW seeks particularly to address the problems of the first set of constraints and to implement the latter. However, the problem is that legal constraints in particular are forever increasing. For example, the inception of the International Criminal Court now brings an individual dimension to International Law, and there is the increasing application of human rights laws, particularly in Europe, which their protagonists seek to promote as an alternative *corpus juris* to the Laws of Armed Conflict.

If this is not difficult enough, mission command is also applied differently across the Services and environments for the following reasons. A maritime force can be defined as having medium mobility. Ships can dash at speeds in excess of 30 knots, but with their auxiliaries overall transit speeds are likely to be in the order of 15 knots. They can be deployed for long durations, they have good connectivity, navies have been in the link business for many decades, and they have a distributed form of command and control with three or four layers from the Maritime Component Commander to individual captains. A useful test of how many layers of command there are is to ask who does an 'estimate', that is receive a mission, analyse it and the constraints and freedoms, and execute or issue orders to a subordinate commander. It is reasonable to suggest that in the case of warships, command therefore stops at the captain, or perhaps the principal warfare officer. While it is normal for a subordinate to analyse his immediate and next superior commanders' intentions, such commanders therefore equally need to think of the implications of their orders two layers down. Therefore, complexity for a Maritime Component Commander is reduced by thinking in terms of tens rather than hundreds of subordinate units or 'moving parts'.

Land forces, however, have low mobility. Notwithstanding the fast armoured dash to Baghdad in 2003, which was then stalled by the need to recuperate and resupply, land forces operate at low speed and for long durations, and due to the constraints of terrain have generally had the worst connectivity, although that is improving. Land forces have multi-layered command and control with six layers between the divisional commander and section commander. A division, of course, in terms of AFVs, guns, tanks etc, has thousands of 'moving parts'. This complexity is reduced by a divisional commander thinking two levels down (ie. in terms of his battlegroups and divisional assets) and thus we are again talking in terms of tens rather than hundreds of 'moving parts', although at the divisional level staff work is far more detailed.

But what of air? Air power assets have very high mobility. Thousands of miles range at seven or eight nautical miles per minute. The downside of this is relatively short duration. The longest F/A-18 sortie during Operation *Enduring Freedom* was over eight hours, and with air-to-air refuelling, aircraft are now generally limited by engine oil consumption, crew limitations or oxygen supplies. Air assets have the best connectivity, not least because of the increased range of communications derived from altitude. It was illustrated earlier with reference to Operation *Iraqi Freedom*, with 2000 offensive and supporting sorties per day, the trend is now towards smaller

and more flexible formations creating thousands of ‘moving parts’ for the commander and his staff to consider. Yet in Operation *Desert Storm*, which was mostly a pre-programmed and highly choreographed air campaign along Cold War NATO lines, there were only two layers of command—the Air Component Commander himself and the package leaders or large-aircraft captains; although some operations were managed on a responsive basis in the current operations cell the vast majority of missions flew to their pre-programmed orders. In this case, the majority of the headquarters was concerned with the process of issuing the orders and the base commanders with providing the resources, the air commander in effect issuing his orders directly to the aircrew. In Operation *Iraqi Freedom*, because of the reactive rather than pre-planned nature of the majority of campaign, a second tier of command emerged, which was either on the operations floor of the CAOC or in an airborne command post, at which the tactical decision to implement the Air Component Commander’s plan was made and orders issued to the aircrew to carry it out. In the air case, however, the complexity is not reduced by introducing additional command layers, which would only slow down the process, but through the apportionment process in terms of the effects they are to achieve (ie. counter air or supporting the Land Component Commander) and then allowing the lower parts of the headquarters to allocate resources to tasks.

The differences in command philosophies between the three environments are driven primarily by physical differences of those environments. The question is, how is mission command going to evolve to be applicable in a net centric environment where the very improvements in connectivity drive greater centralisation of decision-making?

Two examples highlight the potential clash between effects and networks concepts. The first is ISTAR where platforms such as Global Hawk, U2 or the Nimrod R1 are becoming increasingly integrated technologically but, because they are scarce, high value assets, their tasking is becoming more centralised at ever-higher levels and their product is equally being collated centrally. At the other end of the scale there is human intelligence which, while often sourced at very low levels, needs to be rapidly collated and disseminated, again driving a centralised process. The other issue is time sensitive targeting and the coordination of kinetic and non-kinetic mechanisms. As Operation *Iraqi Freedom* showed, the rapid deployment of air power against time sensitive targets is now technologically achievable and those decisions could, in themselves, be delegated to lower levels. However, the requirement to coordinate activities, for example the destruction of a television transmitter prior to broadcasting on that frequency from a Volant Solo C-130, plus the legal and political dimension, also seems to be driving towards centralisation rather than decentralisation. Therefore, net centricity plays into the centralised philosophy of effects-based operations, not least in battlespace management where such issues as the control of airspace and joint fires again reinforces the centralisation trends. So it would seem that the effects-based and net centric approaches are mutually supporting at a basic level of analysis but their conflicts become more apparent as the level of analysis increases. The problems then can be summarised in terms of technology and doctrine, technological disparities being those between components, within components and within coalitions. The assumption of absolute information supremacy could also be net centric warfare’s Achilles heel in the asymmetric world in which we now live. The doctrinal divergences are those within a joint force, that is different environmental doctrines,

the conflict between mission command, the ‘long screwdriver’ and the asset and technology-based division between the United States and the rest. It would seem that the USAF’s view of the CAOC as a weapons system and the British purist mission command view seem to be mutually exclusive and these are exacerbated by diverging attitudes and policies with respect to international law. In summary, then, the main divergence between the net centric and effects-based approaches is that the former seeks to employ a purist view of mission command while the latter requires highly centralised decision-making.

So what, then, are the doctrinal answers and where does it leave Director Defence Studies (RAF) as the man who is currently rewriting our strategic level air power doctrine for the next five to ten years? The first one has to be that it is all about command, and that authority has to be in the right place and not necessarily the lowest; decentralised execution is not an end in itself. Furthermore, it will vary with circumstances and time, the scale of the conflict and the political risk are the key drivers here. Network centric warfare is with us now, we cannot ‘disinvent’ it and we therefore have to embrace it, and in that we are in a transitional period. Although, as an earlier speaker said, whatever the plan is now it will be entirely different five years hence but we still need a plan at least to set us in the right direction.

We should think about the problems in terms of philosophy and principles, not prescription and process, being aware that complex technological solutions tend to drive us down the latter route. Finally, what of the future, and we are considering here the five to ten year time line where doctrine must recognise the realities of the here and now while establishing intellectual conditions for people to move to the next stage. Clearly a major driver here is the development of concepts and technology. The first point is that we have, as far as possible, moved away from deconflicting within a battlespace and are now very much in the era of coordination, whereas NCW takes us further on into integrated operations. What we see is that this integration is not equal, with the Joint Force Commander and Air Component Commanders being the most networked. We are moving towards agile mission groups, where forces are grouped together to undertake a task and then reassigned. This again is nothing new. In air power terms we have been putting together large formations from diverse bases for many years to conduct composite air operations or COMAOs; this was particularly evident in Operation *Desert Storm*. However, it may drive particularly land forces into a more air component-like flatter command and control structure if they are to be flexible. The next point is that land forces are becoming lighter and more mobile, the corollary to this being that air will be even more the major source of firepower in the battlespace, and the battlespace itself will become a single one where the aim of the command and control structure will be to permit rather than prohibit a lot of the components themselves. In a single battlespace it is possible that they will become environmental subject matter experts in a single, and possibly virtual, headquarters. More importantly, their relationships will go away from the current rigid supporting, supported, model into one of mutual interaction and support.

\*\*\*\*\*

## **DISCUSSION**

*Air Commodore Peter McDermott (RAAF – Director General Reserves – Air Force):* In your presentation and the three documents you put up, I thought you made a very telling statement and that was, the fundamentals of air power are much the same for the three major allies, or the three allies that you showed there, but the political differences are the different part. Perhaps, if you take that a little further, you can say that maybe there's another layer that sits on top of that and that is the political layer and we, the national commanders and people who manage those positions, have to look at that. So we're perhaps seeing a confluence, a congruence at that doctrinal level. We heard the previous speaker speak about open systems. Are we on the verge of bringing all of these things together, a brave new world for us being able to work together in our national security endeavour?

*Group Captain Finn:* I think we are and I think we always have been. The point I was making about politics in those manuals was, perhaps, a more narrow one, referring particularly to the Americans where, because of the much greater influence of Congress upon the way they do business, that document actually contains some very politically driven statements. Taking your comment on one further though, and it goes back perhaps also to some discussion yesterday about exercising politicians etc, I find it very difficult to see how we can actually write a doctrine for politicians. I think we can try to educate politicians but I don't think you'll ever, ever lay down a book to say, 'Oh, Prime Minister this is how you go to war'. The interesting dynamic in the United Kingdom, because we've had the same Government now for some seven years and they are actually becoming quite experienced in conflicts, is that they are a more experienced Government than any of the others—you do hear comments occasionally now that the politicians think they know more perhaps than the military advisers—so there is a downside to that. But I don't see how you can ever be prescriptive in the political sense.

*Air Commodore Chris Deeble (RAAF):* I suppose one of the key issues for me, Chris, is the issue of doctrine. You gave it some attributes, in terms of what you expected it to be. One of the concerns that I have is that we don't actually make our doctrine vibrant enough and resonate with our people. We tend to be looking at in lag rather than lead, and to be truly network centric we need to be leading this and building those frameworks into our doctrine. How do you see the change in the way we present it? How do we get our doctrine manual, instead of sitting on a shelf gathering dust, so that all of the people in the organisation can read it and understand the role they play and understand the concepts we need to push forward with?

*Group Captain Finn:* A very interesting question and it is a great problem. How do you sell doctrine to people? It is a wonderful turn-off, except for the 'doctrine geeks'. One of the points I made earlier on though about explaining and understanding is that we need to have levels of knowledge. I think one of the problems we've had—we certainly have it with our current doctrine manual—is that it is very, very dense, it is quite inaccessible intellectually and, therefore, it doesn't appeal particularly to the new entrants, to the new officers and aircrew cadets etc. So you have to look at your target audience and pitch some of it at the explaining level, the simple basic bit, which

is what you've done with your right-hand margin work in the AAP 1000<sup>5</sup>, and then try to blend it on into more detailed coverage. The real point of that is that you can explain to anybody, but you can't actually give anybody understanding. The only thing you can do is to try and interest them and get them to think about understanding. So the approach we're taking in the Royal Air Force is somewhat different from the one you've taken, in that we're actually looking at producing a very small summary manual, AP3001, aimed at the new entrant level and AP3000 will be aimed at the Squadron Leader level when they go into what we're calling the higher Air Warfare Course. The *Air Operations Manual* is going to be the next book in the series and we've also produced an entirely separate book on Air Force history. So we've taken the sort of small book divergence approach, which is very much the way the Joint Doctrine and Concepts Centre is going as well with things like British Defence Doctrine, Joint Vision etc. It really is rather like the eating the elephant joke isn't it; you cut the elephant up into small pieces. But I don't think that you can take doctrine that far forward because if your doctrine books themselves are so far forward—yes, they must have a bit in the back that says these are the steps to the future—if all your doctrine is statements of things you might like to achieve in 20 years, then I don't think it passes the rationality in the here and now test. So it's a very fine balance between sort of getting people to think to the future but actually telling them the core business of today.

*Mr David McIlroy (Air Force Scientific Adviser – Defence Science and Technology Organisation):* You covered the various levels of commanders exercising tactical control and talked about the Bosnian operations. Would you like to comment on whether that might have been driven also by what I understand to be the political dynamics of that particular operation and the divergence within NATO nations of the freedoms that various countries felt they had or hadn't got in conducting that operation?

*Group Captain Finn:* Yes, I think that is very much the case. There is a difference between Bosnia in 1995 and Kosovo in 1999. People say that in Bosnia there was a dual key system. There wasn't. There was a triple key system, because there was a NATO command line, there was the UN line through to Akashi and there was also a national line back to government, so each of the nations participating in that were actually in very close control, and that was due to the scale of the campaign. Kosovo of course was very different. There was the embarrassment of the leakage of the ATO and that, to a certain extent, I think drove the American commanders to there to say, 'Well I can't really trust most of the allies that I'm working with and, therefore, it's going to be very, very American led and very, very centrally controlled'. So there was a very strong political thing in that but more than anything else though I think the main factor was, in fact, the scale of the campaign and because of the connectivity at Vicenza, it allowed the Commander to do it. That's probably the reason why it was so micro-managed, because the Commander, quite simply, could do so.

*Mr Maurice Horsburgh:* I enjoyed your presentation very much sir. My very first Air Power Conference was some time ago, around about 1952, and the keynote speaker was Sir Basil Embery who was CINC of what was then Fighter Command. I

---

<sup>5</sup> AAP 1000 – *Fundamentals of Australian Aerospace Power*, RAAF Aerospace Centre, Canberra, 2002.

remember his opening words almost exactly, ‘We British military planners are frequently accused of preparing for the last war’. Now I’m interested when you mentioned the politicians and the results of political decisions being made. Now there’s no doubt about the last Iraq campaign; it was dazzling militarily, they achieved their aim, but something went wrong in the planning. According to the news this morning, there’s a leaked report from Washington, an intelligence report, that the situation in Iraq is very much worse than the spin doctors would have us believe. So would it be very unkind of me to say that planners, I think I’ll delete military, have now got off to a fine art planning for the last war?

*Group Captain Finn:* I don’t really want to go down the line of yesterday’s question.

*Mr Maurice Horsburgh:* No, it’s not like that, it’s well away from that. I feel that we were heading to introduce democracy to Iraq and, as I say, the military campaign was fantastic but along the planning lines somewhere it has not happened because we were told that the mission was accomplished, but where did it go wrong? I’d like to see a peaceful Iraq, and I’m sure we all would do, but it’s simply not happening, so any comment you have would be very interesting.

*Group Captain Finn:* I share the last concern that you stated but I think it goes back also again to some comments yesterday about how politicians become involved in the application of force. And the DIME—Diplomatic, Information, Military and Economic—are the instruments of power; certainly the way the US sees it. The UK takes a slightly different view on information. What I think we’re trying to do, particularly with the effects-based approach, is at least to allow us at the strategic level to start to consider the interactions of those various levers of power. Now whether that was a reason why Iraq ‘failed’, and I would take issue with that comment, is a different thing entirely. From a military perspective, I think the only thing you can do is take your mission, state the risks involved in how you’ve been told to do it and then achieve that mission. But in the end, political decisions are taken for political reasons. They do not have to be taken only in cognisance of the military realities. So I think that is just frankly the nature of the world that we live in and no more really can I say about it.

*Wing Commander Chris Miller (RAAF – Air Power Development Centre):* Several of the Australian speakers had concerns regarding interoperability with the US, but you didn’t mention it. Does the RAF have the same or a different perspective on interoperability?

*Group Captain Finn:* I think we have exactly the same concerns. I didn’t want to go down the technical route in the presentation, purely because of time, and because I knew most of the other speakers would address technical issues. Interoperability and, more importantly, the financial issues are just as much in the UK mind as anybody else’s.

*Air Commodore Norman Ashworth (RAAF Ret’d):* If I could take the issue back to doctrine and perhaps offer an answer to the one you gave about making the doctrine more meaningful to people. In a few simple words, ‘Keep it simple, stupid’. However, that’s not my question. Really, I’d like to ask you whether you see the basic tenets of air power doctrine changing at all into the future.

*Group Captain Finn:* No I don't think they have because of my argument about fundamental principles and if you put that test on them and they survive then they will continue. I very much come from an evolutionist rather than a revolutionist school on this, which is why I think that those broad building blocks of air power are still very applicable. I suspect they'll be applicable for another 20 or 30 years, at the very least. What do you want to do with air power? You still need to control the air. All right, it is assumed as a given in most campaigns but, maybe, it won't be one day. We still want to achieve strategic effect. We still want to achieve effect within the joint battlespace. We very much want to move to global mobility and the rapid projection of air power. I don't think, at that level, that the fundamental principles are going to change. I think they will endure, as I say, for a good 20 to 25 years. I can't conceive of what will change them in that future, but then that's because I'm conditioned like everybody by the past. It's a sort of epistemic issue really; how do you think. You have to think in the language that you're given, so it is much easier to develop current concepts than it is to actually implement radically new ones. So evolution, rather than revolution is my feeling on that.

# **INFORMATION MANAGEMENT THE KEY TO NETWORK CENTRIC WARFARE**

**AIR VICE-MARSHAL JULIE HAMMER, AM, CSC**

## **INTRODUCTION**

Like our colleagues in other military forces around the world, we have accepted that information is the key to the successful conduct of operations in any theatre of war. It is true irrespective of the capability of the opposing force. It is equally as true of a low level asymmetric conflict as it is of a high-tempo scenario against a technically sophisticated integrated and networked force. Our information capability is critical right across the spectrum of possible conflicts. Acceptance of this premise was inherent in the discussion paper, *Enabling Multidimensional Manoeuvre: The ADF Network Centric Warfare Concept*, released in May this year. The NCW concept highlights that there is both a ‘people’ and a ‘technology’ dimension to networking. A discussion on the ‘people’ aspects would be several presentations in their own right and I suspect that some of the ground has already been covered. I will focus today on how we must capitalise on the capabilities that 21st century technologies bring. We have much to do if we are to enhance collaboration, improve shared situational awareness and support increasingly compressed decision cycles in our new approach to warfighting. This is an outcome that must be achieved by developing the capabilities of the Defence Information Environment, the DIE.

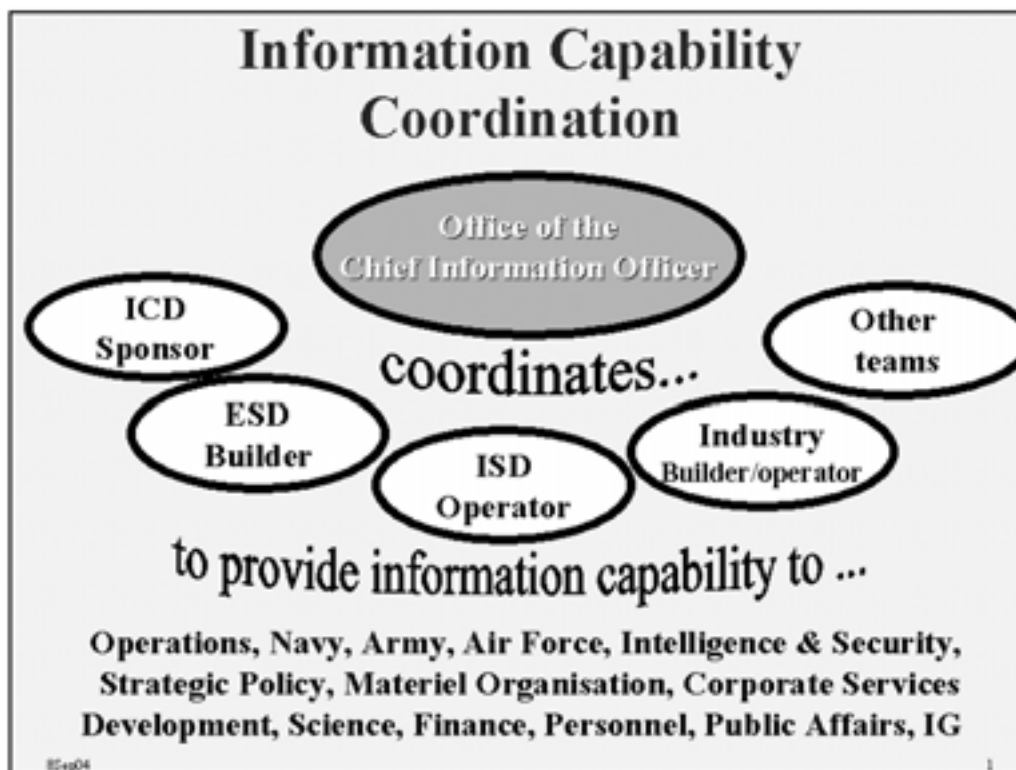
## **MANAGING INFORMATION AS A CAPABILITY**

Whether information is used to plan, conduct and monitor operations, to provide intelligence reporting, to train, prepare and reconstitute forces, to provide logistics support or to support any of the other hundred and one functions performed in Defence, managing information as a capability—just as the Service Chiefs manage the maritime, land and air capabilities—is a critical imperative for us. And of course it is not just our warfighting capabilities that are supported by our information environment. It is also critical to the provision of our support capabilities that enable us to plan and build capability, to administer Defence, and advise and report to Government. One of the things we have increasingly realised, as have most people in the information business, is that information is no longer needed just by one person or organisation for a single function, but by many people and organisations for multiple functions. The requirement for information is all-pervasive and its accessibility must be guaranteed.

The Chief Information Officer (CIO), as the coordinating capability manager of the Defence Information Environment, has the central role in driving the development and management of the DIE and I am pleased to have the opportunity to share with you some of the work that we have been doing in recent months.

In August 2002, the Defence Committee agreed to establish the Office of the CIO to act as the coordinating capability manager for the whole of the DIE. The CIO was tasked:

- to develop and articulate a coherent vision and strategy for the DIE and its components in the form of a comprehensive strategic plan and subordinate plans for each of the discrete capabilities/information domains;
- to coordinate better the information direction of the Defence Groups and the Services;
- to ensure balance in investment in the DIE both for the development of current systems as well as the demands of Force 2020;
- to develop and ingrain the concept of the DIE as a critical enabling component of future warfighting, as articulated in the White Paper;
- with the strategic policy group, to improve joint operational concepts and doctrine for the use of the DIE in future operations;
- to support Strategic Operations Division in their planning responsibilities; and
- to establish robust governance processes for the DIE.



**Figure 1 – Information Capability Coordination**

A new Office of the CIO was formed in December 2002, incorporating the Knowledge Systems Division and other related areas in Defence. As the newly assigned coordinating capability manager for information (or the Defence Information Environment), the Office of the CIO is now responsible for coordinating the activities of the sponsor, the builder, the operator and other teams involved in providing information capability to the fourteen programs within the Department of Defence.

The size of the coordination task is significant. The sponsor (Information Capability Development) consists of a branch sponsoring multi-million dollar capability proposals. The builder (shown as ESD or Electronic Systems Division) consists of a division within the Defence Materiel Organisation buying major information capabilities. The operator (shown as ISD or Information Systems Division) is a large organisation that operates and supports our fixed system infrastructure, as well as continuing to build and evolve large segments of the existing infrastructure. Of course, industry is integrally involved in almost all aspects of the builder and operator roles too. And then there are all the other teams in each of the 14 programs, and particularly the three Services, which currently buy, support and manage parts of the information capability.

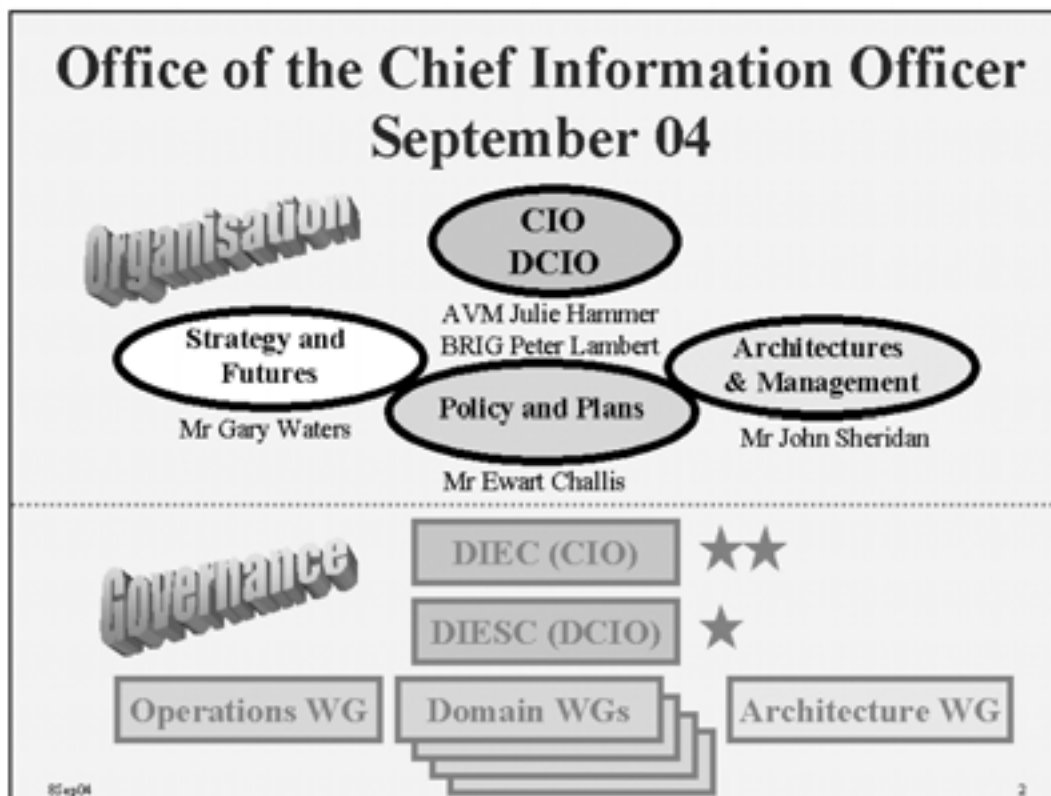


Figure 2 – Office of the Chief Information Officer

The new Office of the CIO was established to put in place strengthened governance arrangements for the Defence Information Environment. Within the Office of the CIO there are three branches. The first branch, Strategy and Futures Branch, deals with strategies and futures, focusing on the time frame of five to fifteen years. This branch is working closely with the Head of Policy Guidance and Analysis to develop the Australian view of network centric warfare. It works to ensure appropriate

information capability investment is introduced into our long-term Defence investment program. The Policy and Plans Branch deals with the issues of capability coordination, prioritisation and convergence in the zero to five year time frame. When necessary it also provides immediate coordination of support to operations. The third branch, Architectures and Management Branch, provides Defence's centre of expertise on architectures and enables the management and governance arrangements necessary to ensure the coordination effort will work.

Governance arrangements have been strengthened with the CIO now providing advice at the highest level as a member of the Defence Committee. Governance is effected through a number of committees and working groups (WGs). With such a complex environment, the key is getting the right people into these forums and picking on the right issues—the ones that make the most difference.

## **THE DEFENCE INFORMATION ENVIRONMENT**

One of our greatest challenges has been dealing with the fact that the DIE itself was not a well-defined or well-understood entity. We frequently found that we were talking at cross-purposes with each other, with our key Defence stakeholders, and with industry. This reflected our different backgrounds, different operational experience, and different levels of technical understanding. It was clear that to move forward in development of the DIE, we needed to define it in terms that were comprehensible as well as comprehensive. We needed to develop a DIE Framework that provides us with the basis for discussion. As coordinating capability manager, the CIO has taken the lead in this endeavour. Specifically, we have been attempting to address a range of perceived and actual deficiencies as follows:

- There were no agreed boundaries of the DIE.
- There was no common description of the components that comprise the DIE.
- There was no widespread understanding of technologies involved.
- There was no widespread understanding of information management issues.
- There was no coherent vision of the DIE that we seek in the future to underpin the NCW Roadmap.
- We had no way of measuring the performance of the DIE, or any changes we made to it.

Effectively, we did not have a common language to discuss the DIE. Little wonder, therefore, that we were often heading in different directions.

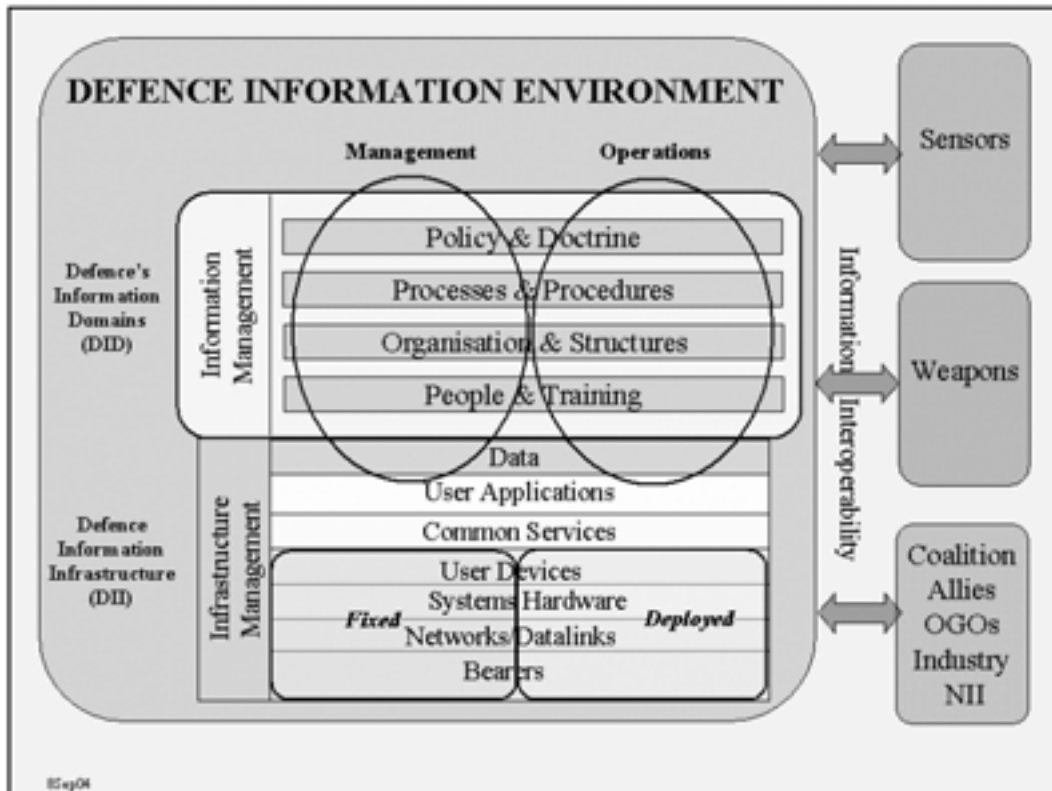


Figure 3 – Defence Information Environment

The development of the DIE Framework, shown in Figure 3, began in the Office of the CIO about a year ago and while it has been widely disseminated and discussed, it continues to be ‘work in progress’. We are continuing to finetune it as our conceptual thinking grows. Nevertheless, it can be regarded, however, as authoritative, although evolving. It clearly identifies that the DIE is much more than infrastructure. It identifies another major segment, simply called ‘Defence’s Information Domains’ on the Framework, which describes the components of the user dimension that interact with the infrastructure. These components—policy and doctrine, processes and procedures, organisations and structures, people and training—are what are called ‘Fundamental Inputs to Capability’ in our Future Warfighting Concept. It identifies ‘Information Management’ as the function that coordinates all of these components, in the same way that ‘Infrastructure Management’ coordinates all aspects of the infrastructure. The Framework identifies the important interfaces to entities external to the DIE, such as our allies, other government departments and industry, as well as to other systems, such as sensors and weapons systems. Interoperability with these external entities is a critical aspect of DIE capability, just as it is a central element of NCW.

### Defence Information Infrastructure

We need to be able to drill down into the DIE Framework to talk at greater and greater levels of detail. We have already begun this exercise for the Defence Information Infrastructure and have produced a useful representation (Figure 4), which supports both technical and non-technical discussion.

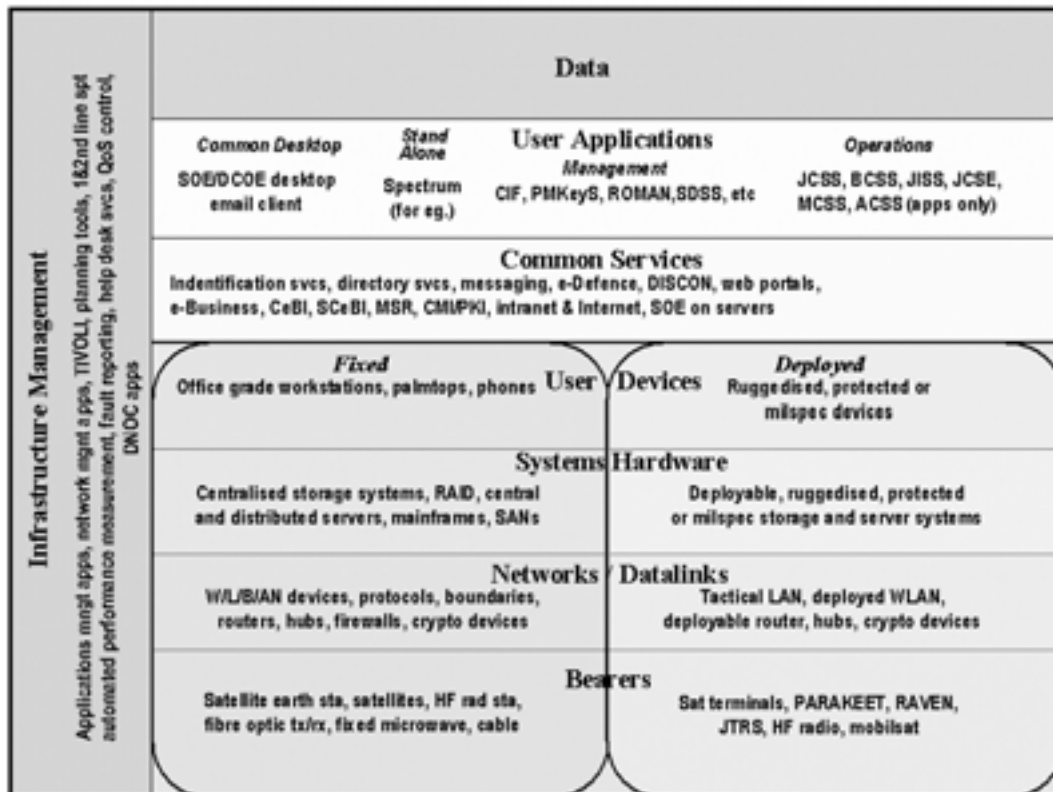


Figure 4 – Infrastructure Management

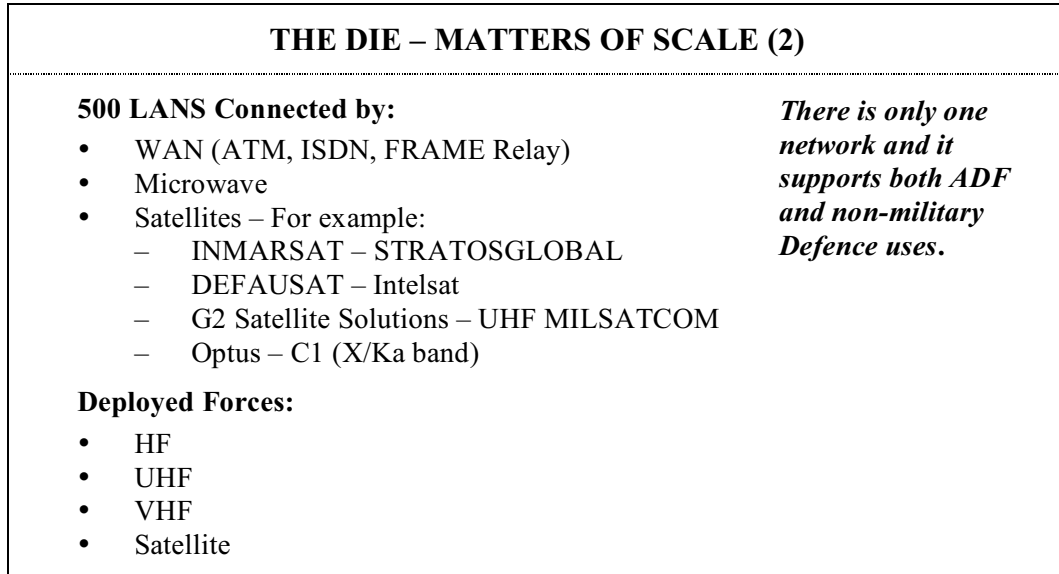
With regard to this infrastructure, it would be useful at this point to give you some specifics about the size and scale of the DIE. The following tables (Figures 5–8) provide some illuminating facts and figures.

<b>THE DIE – MATTERS OF SCALE (1)</b>	
<b>Restricted Network</b>	
• Users	85,000
• Desktops	92,500
• Servers	1,000
<b>Secret Network</b>	
• Users	85,000
• Desktops	92,500
• Servers	1,000
<b>Voice Services</b>	
• Users	85,000
• Desktops	92,500
• Calls / Month	4,250,000

Figure 5 – DIE Connections

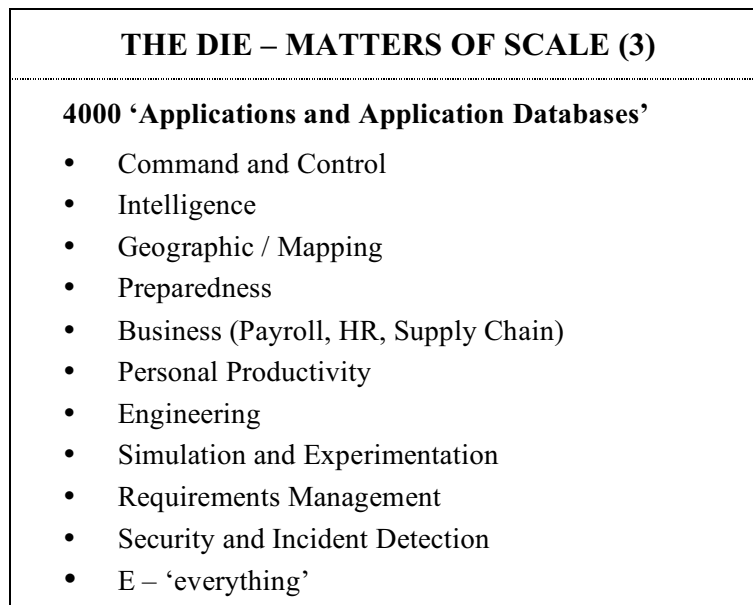
The details in Figure 5 are for Defence’s Restricted and Secret Networks only. I will not be going into details for the Top Secret Network. As you can see, Defence

manages arguably the largest and most complex information environment in Australia. It connects some 98,000 users in about 650 locations, including 35 overseas sites and 29 deployed elements. It manages its own communications bearers, which transport voice as well as data services.



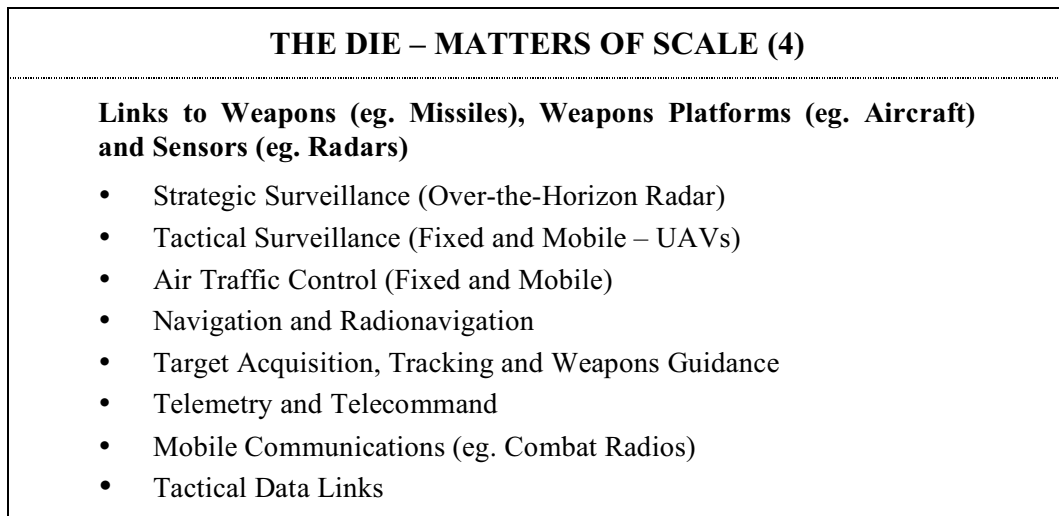
**Figure 6 – DIE Support to Users**

The DIE supports fixed and mobile users, staff in headquarters and on bases as well as deployed forces overseas and afloat. The communications layer was consolidated almost ten years ago and the IT layer several years later after the establishment of Information Services Division following the Defence Efficiency Review. Effectively, we have only one network at each security classification—a notable achievement.



**Figure 7 – Applications and Application Databases**

The DIE supports approximately 4000 applications and applications databases spanning both warfighting and management. Their functionality would reflect that of the sum of every other Commonwealth department, and then some more.



**Figure 8 – Links to Weapons and Sensor Systems**

As shown in Figure 8, the network must not just inter-operate with other networks. It must also connect and communicate with complex weapons, weapons platforms and sensor systems for the exchange of a myriad of different types of information.

## Defence Information Domains

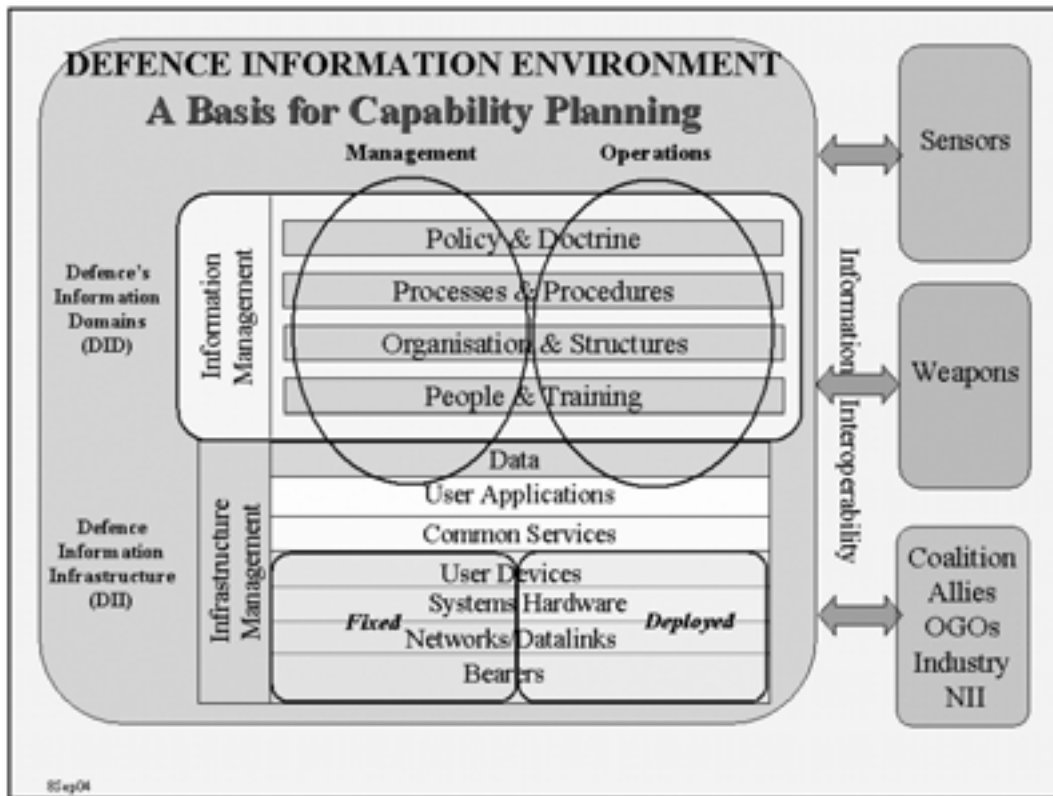


Figure 9 – A Basis for Capability Planning

While it may be a challenge to come to grips with the size and complexity of our information infrastructure, this is a comparatively simple issue when compared with the complexity of managing our Information Domains. The top half of the diagram at Figure 9 reflects the Information Domains and I colloquially refer to this as the ‘user space’. We have found that this is most usefully conceptualised in terms of our Enterprise Processes. This provides us with the most useful mechanism for capability planning.

In March this year, we took a proposal to the Defence Committee seeking agreement to the set of Enterprise Processes shown in Figure 10. This approach reflects that users interact with the infrastructure through processes that involve utilising software applications. Enterprise Processes are those that are conducted by more than a single group within Defence and which need to be undertaken consistently across the whole organisation. If we are to improve the efficiency and effectiveness of our processes, the information systems that support them and the associated data repositories, then we must take a whole-of-enterprise approach to our processes.

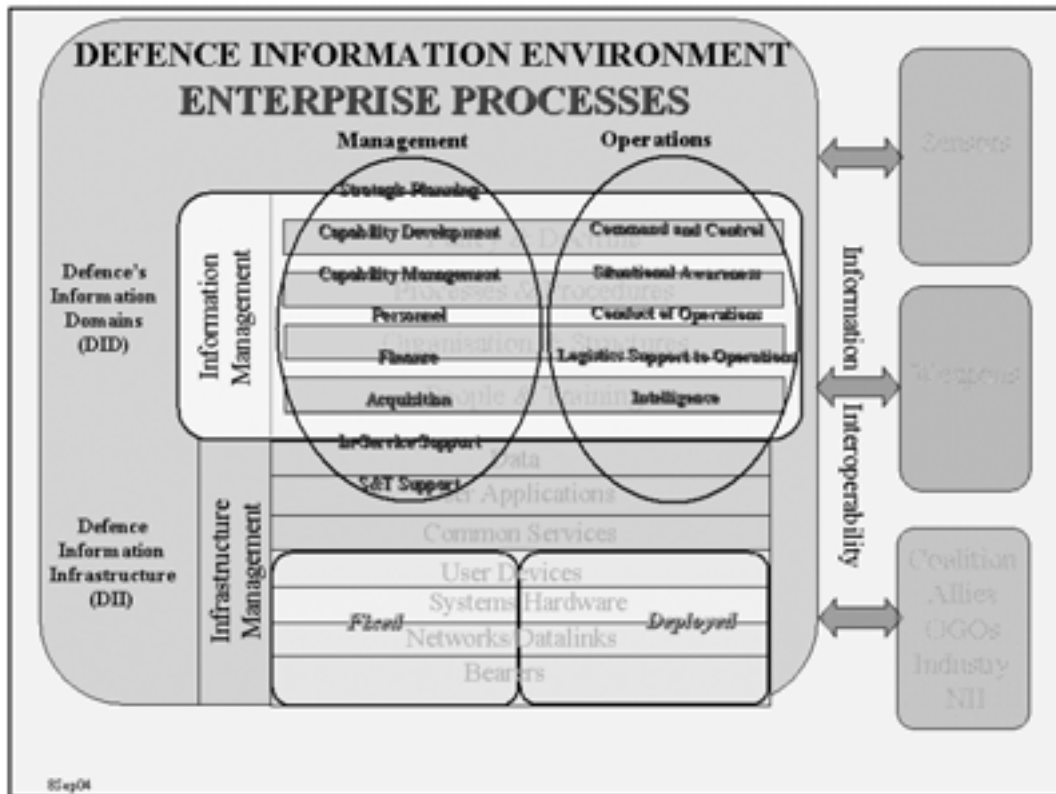


Figure 10 – Enterprise Processes

The Defence Committee, in providing ‘in principal’ agreement to these Enterprise Processes, also agreed an Enterprise Process Owner at the Defence Committee level for each one in both the Management Information Domain and the Operations Information Domain. These Enterprise Process Owners are shown in Figures 11 and 12:

<b>MANAGEMENT INFORMATION DOMAIN – ENTERPRISE PROCESSES (AND ENTERPRISE PROCESS OWNERS)</b>
<ul style="list-style-type: none"> <li>• Strategic Planning (DEPSEC S)</li> <li>• Capability Development (CCDG)</li> <li>• Capability Management (CN, CA, CAF, CIO, DEPSEC I&amp;S, DEPSEC CS)</li> <li>• Personnel (HDPE)</li> <li>• Finance (CFO)</li> <li>• Acquisition (CEO DMO)</li> <li>• In-Service Support (CEO DMO)</li> <li>• Science and Technology Support (CDS)</li> </ul>

Figure 11 – Management Information Domain – Enterprise Processes

<b>OPERATIONS INFORMATION DOMAIN – ENTERPRISE PROCESSES (AND ENTERPRISE PROCESS OWNERS)</b>
<ul style="list-style-type: none"><li>• Command and Control (CJOPS)</li><li>• Situational Awareness (CJOPS)</li><li>• Conduct of Operations (CJOPS)</li><li>• Logistics Support to Operations (CJOPS)</li><li>• Intelligence (DEPSEC I&amp;S)</li></ul>

**Figure 12 – Operations Information Domain – Enterprise Processes**

Happily, it has been possible to identify a single Enterprise Process Owner for each process, with the exception of Capability Management (Figure 11) where we have a number of instances of this process being performed independently. We are currently undertaking work to examine how similar each instance of the Capability Management Process is.

The Defence Committee agreed roles and responsibilities for each of the Enterprise Process Owners are as follows:

- **describing their Enterprise Process** in accordance with the method agreed by the Defence Information Environment Committee (DIEC);
- **identifying sub-processes and owners** for their Enterprise Process;
- **controlling their Enterprise Process** and its interactions with other processes;
- **consulting with the various Defence Groups and the Services** to ensure that the Enterprise Process supports their requirements;
- **agreeing functional requirements for the information systems** that support their Enterprise Process—and I would emphasise ‘functional requirements’ not ‘technical specifications’;
- **defining the skills and competencies** associated with their Enterprise Processes for inclusion in relevant training programs; and
- **contributing to overall DIE planning.**

The CIO also has a set of roles and responsibilities in this construct to provide an overarching governance framework in which all of the Enterprise Process Owners will be supported, the interaction between their processes managed, and their requirements and priorities included in overall DIE planning. The CIO roles and responsibilities are as follows:

- establishing and maintaining the **governance arrangements for Enterprise Processes**;

- establishing, and gaining DIEC agreement to, a **method for describing Enterprise Processes** consistently across Defence;
- providing the necessary **subject matter expertise** to Enterprise Process Owners to support the description of Enterprise Processes;
- **identifying and resolving inconsistencies between Enterprise Processes** or raising those inconsistencies to the appropriate forum for resolution;
- **including the Enterprise Process Owners in the DIE planning process**; and
- ensuring that the **priorities for Defence Information Infrastructure development** support the Enterprise Processes.

We have discovered that one of the key enablers for the effective coordination of the information capability is a robust architectural practice. Architectures are the mechanism which allows us to describe what we have in the ‘user space’ (the Defence Information Domains) through enterprise architectures and in the ‘infrastructure space’ (the Defence Information Infrastructure) through system and technical architectures. We have developed a Defence Architecture Framework, based on the US model, and over the last year or so we have started to populate that framework. Most of our recent work since the March Defence Committee meeting has been to work with the Enterprise Process Owners to begin the description of their processes through this enterprise architecture approach.

We have also progressed well with the capture of explicit technical architecture standards, such as common and standard operating environments, a technical reference model for the DIE, combined interoperability technical standards and an approved technical standards list. As we develop the enterprise architectures through a federated model, we are beginning to develop a better picture of the enterprise systems portfolio, but we are still some way from having a mature and evolving architectural practice.

## **VISUALISING THE FUTURE THROUGH INFORMATION ARCHITECTURES**

A recent important development has been the establishment of the NCW Program Office in the Information Capability Development Branch within Capability Development Group. The aim of the NCW Program Office will be to ensure that information aspects are coordinated between all projects within the Defence Capability Plan (DCP), whether those projects be those that directly affect the DIE (such as command support or communications systems projects) or projects that will have an impact on the DIE in some way or another. In truth, there are very few projects that do not fall in the latter category. Every platform project, such as the Air Warfare Destroyer or the Joint Strike Fighter, will have systems that must interface and inter-operate with the DIE, providing information to it, drawing information from it, or communicating through it with other platforms and systems. Every weapon or sensor system project will similarly be affected.

The initial focus of the NCW Program Office will be to work with the CIO to develop a more comprehensive understanding of the ADF’s current information architecture, to develop a description of the architecture we seek for 2010 and 2020, and then to assess the architecture that will be achieved if we proceed exactly as planned with all our current projects. For existing projects, it may be that we find some adjustment is warranted and we will need to assess how practical that is to achieve. For new projects, there will be a future architecture providing the guidance within which they must develop their specific capability. There is much work to be done, and it must be done quickly, if we are going to assure alignment across the whole Defence Capability Plan.

As a further aid to conceptualising the future, we have developed a set of attributes (Figure 13) by which we will describe our information environment, both the information domains and the infrastructure.

<b>DIE ATTRIBUTES</b>	
<b>Commander / Customer</b>	<b>Supporter / Supplier</b>
<ul style="list-style-type: none"> <li>• Functionality</li> <li>• Interoperability</li> <li>• Useability</li> <li>• Pervasiveness</li> <li>• Reliability</li> </ul>	<ul style="list-style-type: none"> <li>• Governance</li> <li>• Security</li> <li>• Survivability</li> <li>• Surge</li> <li>• Adaptability</li> <li>• Quality</li> <li>• Sustainability</li> <li>• Standardisation</li> <li>• Efficiency</li> </ul>

**Figure 13 – DIE Attributes**

We have used these attributes to describe in very broad terms the current states of the DIE; as well our aspirational visions for the DIE of 2010 and 2020. These aspirational states have been recorded in the DIE Strategic Intent and will inform the architecture work that we are embarking on with the NCW Program Office. From the DIE Strategic Intent, and from detailed examination with a wide range of stakeholders, we have distilled into a Defence Information Infrastructure Plan some of the critical and urgent actions on which we must focus our attention. What has yet to be done is to develop performance measures for these attributes so that we can quantify the different DIE states that we are describing and measure our progress towards achieving them. We are currently working on this.

I have described how the development of the DIE Framework has formed a basis for the Enterprise Process and Enterprise Architecture work that is providing a structured approach to our Strategic Planning of the DIE. We are looking at information management through an enterprise process approach, based on the Enterprise Processes approved by the Defence Committee at its meeting in March 2004. We are doing our infrastructure planning through a systematic look at each layer of the

infrastructure as depicted in the Framework. Together, this has enabled a logical structure to our thinking and our planning. But the DIE Framework has provided a useful lens through which to view several other major initiatives that have recently provided a new vision for the future.

Three separate but closely related and concurrent studies have recently been undertaken to review the funding, governance and organisational arrangements for the DIE. The Baseline Funding Review was conducted by a small team within the CIO Group to identify planned expenditure on the DIE across the whole Defence portfolio over the next ten years. The Inspector General's Evaluation of DIE Governance examined current governance arrangements and made recommendations for improvement. The Review of DIE Organisational Arrangements was conducted by the Boston Consulting Group and looked at organisations responsible for the strategy, planning, development, implementation and support of the DIE. The recommendations of all three reports were considered at an extraordinary meeting of the Defence Committee on 13 August 2004.

### **Baseline Funding Review**

The first phase of the Baseline Funding Review ran from January to July this year. With the support and assistance of all of the Defence Groups and Services, it collated planned expenditure across the portfolio. For this exercise, it was necessary to constrain our scope to looking at Unclassified, Restricted and Secret Networks only, excluding the deployable systems that form part of the DIE, and also excluding the Top Secret Network. Funds have been broken down across the infrastructure layers of the DIE: bearers, networks and data links, systems hardware, user devices, common services, user applications and data. Delineation between sustainment, investment and workforce costs has also been achieved. This has provided us with a perspective that we have never had in the past. The key findings of the Baseline Funding Review are shown in Figure 14.

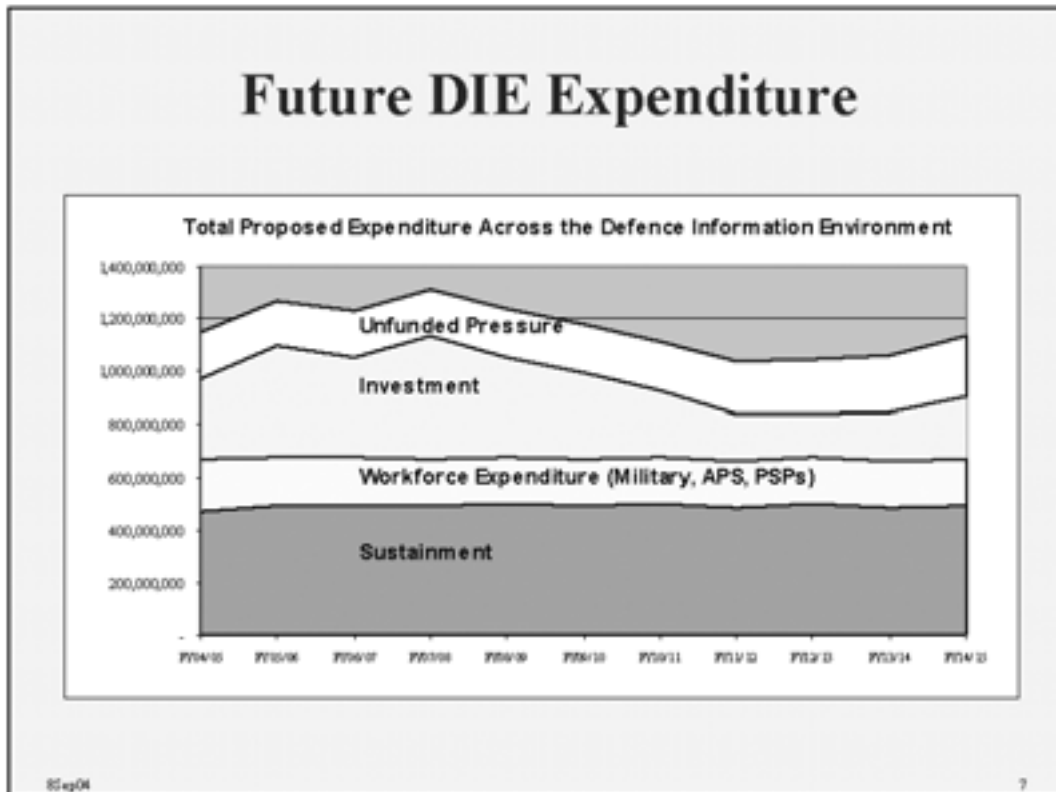
<b>BASELINE FUNDING REVIEW KEY FINDINGS</b>	
<ul style="list-style-type: none"><li>• <b>Gross acquisition value of approximately \$1.1b</b><ul style="list-style-type: none"><li>– (\$810m in hardware and \$281m in software)</li></ul></li><li>• <b>Net book value of approximately \$551m</b><ul style="list-style-type: none"><li>– after depreciation</li></ul></li><li>• <b>Annual expenditure of approximately \$1.1b</b><ul style="list-style-type: none"><li>– \$490m sustainment, \$390m investment and \$183m workforce</li></ul></li><li>• <b>Annual Expenditure is 6.5 per cent of the Defence Budget</b><ul style="list-style-type: none"><li>– comparable to anecdotal figure for US Department of Defense</li><li>– comparable to major commercial enterprises</li></ul></li></ul>	

**Figure 14 – Key Findings of Baseline Funding Review**

We now know that we are managing assets with an original acquisition value of a little over a billion dollars, almost three-quarters of which comprise hardware assets.

From an accounting perspective, this reduces to a net book value of a little over half a billion, noting that almost all of our desktop infrastructure costs are written off in the first year. Our annual expenditure comprises about 6.5 per cent of the Defence Budget, a figure that we hope to benchmark against other military forces in the future. This is in the same ballpark as major civilian enterprises, which vary between six and twelve per cent, depending on the degree to which the industry sector is technology focused.

**Future DIE Expenditure**



**Figure 15 – Future DIE Expenditure**

Aggregated information provides a surprisingly consistent picture out across the ten years of the Defence Management Financial Plan (DMFP). Not surprisingly, planned investment tapers off in the outer years, but this is most likely a reflection of the difficulty in planning for this type of capability more than five years out. It reinforces the need for us to conceptualise the future DIE better and ensure that capability requirements are programmed for investment. An additional challenge will be to reduce the cost of ownership of the DIE to ensure that currently unfunded sustainment pressures can be accommodated within existing budget levels.

**Proposed DIE Expenditure by Component**

Our proposed expenditure, as broken down across the layers of the DIE, brings no great surprises (Figure 16). Our bearer costs, encompassing significant satellite and fibre costs associated with our terrestrial and overseas communications network, as well as the total cost of Defence’s spectrum usage, are a realistic 23 per cent. Network

and data link costs at 18 per cent tend to be a function of the number of sites we support, and user devices at eight per cent are dependent on the number of users we have. Expenditure on our 4000 applications and applications databases comes in at 28 per cent and to some degree impacts on the cost of systems hardware at 15 per cent. This is an area that warrants some intense scrutiny and rationalisation into the future. We will be working on this in conjunction with the agreed Enterprise Process Owners. A significant challenge for us will be to determine whether this is the right level of expenditure on each DIE component.

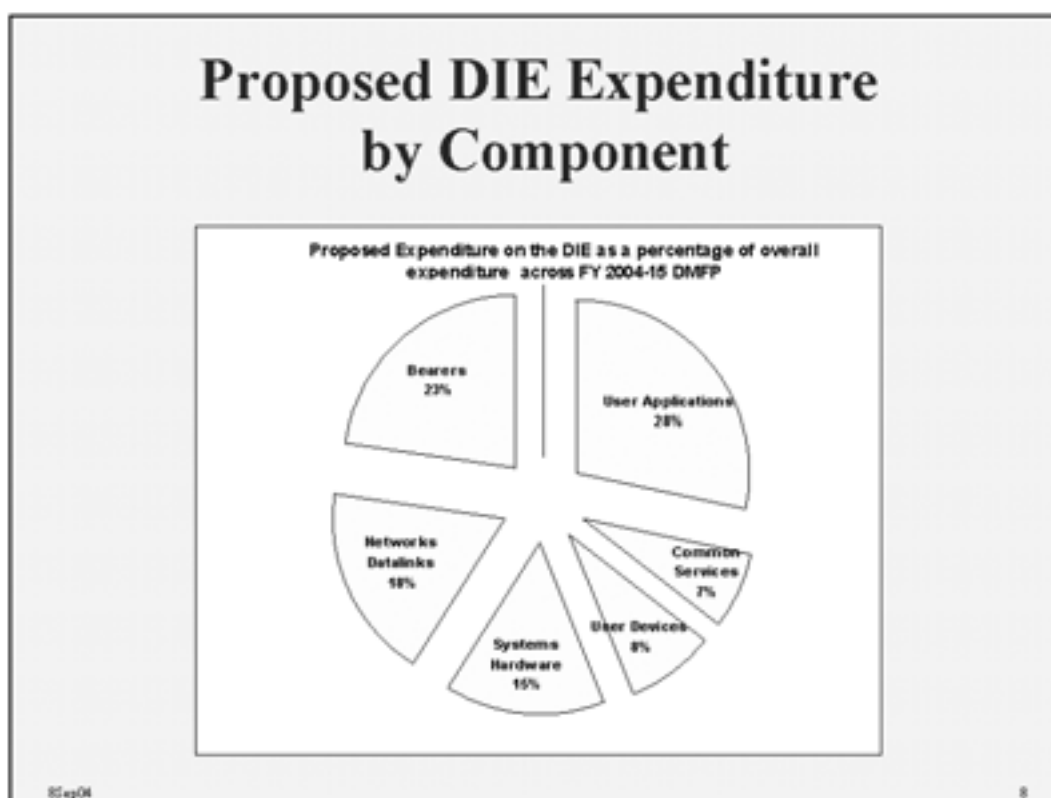


Figure 16 – Proposed DIE Expenditure by Component

## Governance

The Inspector General's evaluation of DIE governance found that the approach established by the Office of the CIO provided a sound basis and should be further developed and extended. In particular, it endorsed the approach of governance through a hierarchy of Enterprise Processes and Enterprise Process Owners, and strongly supported the documentation of these processes through enterprise architectures.

## Organisation

The Inspector General's findings were closely aligned with those of the Review of DIE Organisational Arrangements conducted by the Boston Consulting Group. The Boston Consulting Group further went on to recommend that a number of the organisational elements responsible for planning, development and operations of the DIE be brought together under an expanded CIO Group.

New organisational arrangements for the DIE were agreed at a meeting of the Defence Committee on 13 August 2004. Specifically, the current Office of the CIO and Information Systems Division will be amalgamated to form the core of the new expanded CIO Group. Also to be transferred into the new Group are the software development and support functions of a number of the management enterprise applications. Finance and personnel applications development will transfer from the Chief Finance Officer (CFO) and Head Defence Personnel Executive (HDPE) respectively by the end of the year. Logistics applications development will remain with the Defence Materiel Organisation (DMO) to ensure that the Standard Defence Supply System (SDSS) Get Well Program is not disrupted, and this will be reviewed in July 2006. The full range of enterprise applications being developed within the organisations of the Enterprise Process Owners is yet to be fully scoped but this will be done over the next several months. Staff associated with specifying functional requirements for the enterprise applications will remain with their Enterprise Process Owners; only technical staff will transfer to the expanded CIO Group. Our new governance arrangements need to ensure that we have strong linkages between ourselves and the Enterprise Process Owners to make sure that we deliver to their functional requirements.

An important aspect of achieving an affordable and effective DIE in the future is the rationalisation and standardisation of suites of applications, which support a particular enterprise process. The Baseline Funding Review, in conjunction with the newly fielded 'discovery tool' within ISD's System Management Product, Tivoli, will provide us an unprecedented insight into the diversity and the cost of applications support. The CIO will work with Enterprise Process Owners to formulate rationalisation strategies for applications within their remit.

Another important aspect is maintaining visibility of expenditure on the DIE that has been afforded by the Baseline Funding Review. A follow-on task for the team will be to extend the review to cover deployable systems and the Top Secret network. All such funding, whether it be for sustainment or investment, will in future be managed as a program across the portfolio under the supervision of the CIO. Expenditure in accordance with portfolio priorities will be approved each year in the context of the DMFP. Groups and Services will work together with the CIO to ensure that all of their expenditure accords with the DIE Strategy and Plan, and DMFP agreed priorities.

So in reflecting on all these recent initiatives, what is it that we are trying to achieve? Our aim is to achieve:

- a common understanding about what we consider to be within the DIE and what consider to be outside it;
- a means of consistently describing the components of the DIE;
- a coherent vision of the DIE we seek in the future in terms of the DIE Framework and its attributes, documented in enterprise, systems and technical architectures;

- agreed strategies and a detailed plan to achieve that DIE vision;
- a means of measuring the performance of the DIE in terms of its attributes and measuring our progress towards the future vision;
- closer linkages between strategy and planning, and development, implementation, support and operations through closer organisational arrangements and stronger governance;
- greater visibility of expenditure on the DIE;
- portfolio level prioritisation and control of expenditure; and most importantly
- **an efficient and effective DIE capable of supporting Defence's warfighting and management functions.**

In summary, if we want to move forward to a more network centric future, there is no doubt in our minds that we must view information as a capability in its own right. As a result:

- we are developing a single DIE with a single point of accountability;
- we are managing information as a capability;
- we are leading development of the DIE through future warfighting concepts (including network centric warfare) and through experimentation; and
- we are supporting decision-making through sound business processes, as analysed and developed within a Defence Architectural Framework.

So as you can see, there is much happening on every front of the DIE. The next few years will be an exciting time as we move forward into the new organisation with strengthened governance arrangements and a portfolio program management approach to funding and expenditure. Under these new arrangements, there is an urgent imperative to improve efficiency and effectiveness of the systems and reduce the ongoing cost of ownership. There is no question that we must be successful in this endeavour if we are to achieve the network centric capability to which we aspire.

\*\*\*\*\*

## ***DISCUSSION***

*Squadron Leader Blake Barrett (RAAF – Defence Materiel Organisation):* My question relates to the DIE and its relationship to network centric warfare. The DIE has been around for a while now, probably two or three years. You said in your presentation that you're still developing the performance measures for some of the operational aspects, for example, interoperability. I was just wondering if you might

be able to expand on some of those performance measures. I realise that they're still in development but could you give just some of the details ma'am?

*Air Vice-Marshal Hammer:* Well, they were on one of the earlier slides. We're trying to focus on attributes and describe attributes in terms of performance measures, and we believe there are two types of attributes of the environment. There are those that are of concern to the operational commanders or, if I could fall back into that business speak, the Enterprise Process Owners because a lot of the people we need to support in Defence are the people doing the day-to-day administration of Defence, as well as the warfighting side of the house. So they're, if you like, our customers, our commanders who have particular requirements of the DIE. Most of what they require is functionality and a capability that they can see as a commodity. They actually want to be able to take for granted the services that the DIE provides. They want it to be there. They want it to be ubiquitous and they want it to be like turning on a light switch—it turns on when you come into the room and that's the last you have to think about it, because it delivers the light that you need to do your work. We need to deliver the services of the DIE in the same way. So the attributes that the commanders are interested in are a different set of attributes to those that the supporters of the system are interested in, and that's the second group. The attributes associated with how well the DIE performs on a day-to-day basis are the attributes that are of interest to people like DMO, because they're having to deliver those sorts of systems, and Information Systems Division who are having to support and operate the DIE. They're things like: it's sustainable, it's reliable, it's able to surge to meet a contingency operation, it's got redundancy. We haven't yet actually worked out performance measures associated with those. A couple of months ago I spent some time with my colleagues in both the UK and the US, and we are all very interested in developing those sorts of performance measures. We're all at slightly different stages of doing so, but none of us believe we've really got a good framework in place yet. So that's work in progress.

*Wing Commander Peter Spiess (RAAF – Air Combat Group):* I'd like to take you to task a little bit about information management and your comment that information is a capability. I personally think that information distribution is obviously a key to network centric warfare and it is a key to many other aspects of the military. However, I don't think information is a capability at all. I believe that knowledge or wisdom is, in fact, the capability that we're after and there seems to be a lot of investment going into information distribution, but what about the distilling of information into wisdom?

*Air Vice-Marshal Hammer:* I think that's a really good point and your perspective is included in the way in which I think of information as a capability. Unless we can distribute the information to the people who need it, then they can't do their warfighting or their administrative role, so it is a capability in that sense. But what you're looking at is how we actually think about capturing intellectual capability, capturing the learning and making us into a more agile organisation so that we actually don't lose the knowledge of our experience as we move forward. We're doing a bit of work on that in Gary Water's Strategy and Futures area. We're examining what actually is intellectual capital. How might we characterise that? How might we understand it better so that we might be able to measure it and might be able to capture it and not continue to lose it? We're also doing a little bit of work with

Toffler Associates on what makes an organisation agile, what makes an organisation a learning organisation and what allows us to actually take information and convert it into knowledge and wisdom that we don't lose. So, it's a really good question. It's a very important aspect and I'd like to thank you for bringing that up because I didn't touch on that dimension and it is one that we're looking at but it's one we don't have any answers for yet.

*Air Vice-Marshal Eric Stephenson (RAAF Ret'd):* As a former Director General of Air Force Health Services, it's a matter of concern to me that a lot of the younger people these days rapidly develop a form of depression when they get into the military. Something that's come across in the last couple of days, beyond all doubt, is that NCW is going to be essential, probably, to our survival as a culture. I don't think I am overstating the case. Is there not also a case, in terms of information, that we should go to the Minister of Education, not just Defence, and say, 'Isn't it about time that you started teaching about these things in the schools?' The educationists will scream 'blue murder' but, if our survival may depend on it, I think there's a case for beginning pretty early on. Professor Babbage made this point yesterday when he talked about total educational component in our society.

*Air Vice-Marshal Hammer:* A lot of our young people in the schools certainly understand the technology dimension but, if I understand your point correctly, it's more about understanding what that technology can enable groups that are involved in terrorism actually to achieve and sensitising our young people to that and making them more aware of the things they need to understand to be able to deal with this in the society in which we live. All I can say is that I agree with you. I think that would be a sensible approach to bring into the schools but I'm not sure at what stage—you probably need to be an educational psychologist to look at that.

*Air Vice-Marshal Stephenson:* That is exactly what I was meaning. They should be made aware of what the military can offer them and expand their horizons to, simply through information technology.

*Air Vice-Marshal Hammer:* Indeed.

# THE FUTURE OF THE NAVY AND NETWORK CENTRIC WARFARE

## VICE ADMIRAL CHRIS RITCHIE, AO, RAN

It is my pleasure to address the 2004 Air Power Conference, and I thank Air Marshal Houston for this opportunity to tell you about the future of the Navy and Network Centric Warfare (NCW).

I would like to take my lead from two American officers who had a great deal to do with winning the war in the Pacific from 1942 to 1945, Fleet Admiral Ernest King and General Douglas MacArthur. And I would be so bold as to draw some similarities between me as Chief of the Australian Navy in 2004 and Admiral King as US Chief of Naval Operations in 1942. King's daughter said of him:

He is the most even-tempered man in the Navy—he is always in a rage.

Actually, that is not the comparison I am seeking, but rather it is with King's own words to a Staff Officer in 1942, when he said:

I don't know what the hell this 'logistics' is that Marshall is always talking about, but I want some of it.

I feel the same way about NCW, and Angus Houston has put me on the spot by asking me to talk about it for 35 minutes and to answer questions! So I turn to General MacArthur for inspiration. Half a century or so ago, MacArthur said:

New conditions require, for solution—and new weapons require, for maximum application—new and imaginative methods. Wars are never won in the past.

Today the 'new conditions' that we face, in the form of threats to peace and security in our strategic environment, have multiplied in complexity and uncertainty. And the 'new weapons' that we face range from weapons of mass destruction and missile proliferation to the use of relatively crude, simple and inexpensive weaponry that can be used to apply intense pressure.

One of the new and imaginative ways of the future, in which we will combat these new conditions and new weapons, will be network centric warfare. Today I am going to paint a picture for you of Navy's vision for network centric warfare and what we are doing about achieving the vision.

As I was preparing today's presentation, I admit to being less than comfortable in the fact that I knew what our vision was and where we are going. But that has been resolved. It also dawned on me that I have little insight or appreciation into what my Air Force and Army counterparts think on this matter. This is one of the first challenges we in the ADF face—unifying what we in all three Services see as our ultimate NCW goal. This conference, however, represents a leap forward in the path

to unifying our visions, as most importantly does the formation of the Network Centric Program Office.

On the surface, one thing we all have in common is our mutual sufferance of unavoidable fashionable jargon from the network centric lexicon. We hear terms such as seamless, fusion, battlespace, grids, bandwidth, multi-dimensional manoeuvre, mission command and self-synchronisation used endlessly, and often meaninglessly. Indeed, I suspect that some of these concepts will have wormed their way into my speech today. So keep the questions simple!

But for me, most of these terms are incidental to what network centric warfare is all about—it is all about knowledge. René Descartes got it right a couple of hundred years ago when he said that ‘knowledge is power’. The more we share the knowledge that Navy, Army and Air Force are all so diligent in collecting, the more power we will have as a force working together.

But back to Navy’s vision for the future and NCW. The RAN of the future will place an even greater emphasis on selective high technology systems than it does now. We will capitalise on advances in information technology to link sensor grids, databases, models, weapons grids and weapon delivery platforms. This will enable Navy to conduct seamless combined operations as part of a networked ADF. This will also enable Navy to conduct seamless joint operations with the US and other key allies. For such operations where interoperability will be vital, we must ensure that our innovations in NCW have highly compatible technologies and common standards with those of our allies.

Through high technology we will achieve knowledge superiority, which will entail a vastly improved understanding of the battlespace and the ability to coordinate widely dispersed maritime force elements to ensure that their actions are harmonised. Our situational awareness and enhanced battlespace resolution will lead to increased cooperation and coherence between staff in our headquarters, which will facilitate decision superiority. The common operating picture that NCW will provide will enable a quickening of the exercise of command, and raise operational tempo. It will also result in increased survivability and lethality, the latter through more effective and responsive targeting.

But NCW involves a major cultural change beyond information superiority about the battlespace in which we are operating. NCW involves a cultural change in the way warfare is conducted by following several lines of development. We must address the human dimension through leadership, personnel culture, training and organisation. We must address our doctrine through changes to our processes, tactics, techniques and procedures. And we must ensure that we have the technology and facilities to employ the future warfare fighting concept of multi-dimensional manoeuvre, both jointly and with our allies.

I am sure that most of you have heard of the famous case of the USS *Yorktown*, a state-of-the-art, guided missile cruiser with an Aegis weapons system. *Yorktown* had the benefit of being fitted with an array of commercial off-the-shelf computer workstations using Microsoft Windows NT for ship control and other functions. Off Cape Charles, Virginia one day in September 1997, a control systems operator

mistakenly entered faulty data into a database. His error crashed the program and set off a cascade of system failures throughout *Yorktown's* electronic control systems that ultimately caused its propulsion system to fail. One of the US Navy's most powerful of warships was left dead in the water.

Of course, this is not NCW, but is indicative of the pitfalls and challenges that lie ahead for the NCW transformation of warfare. I like to think that for Navy, however, it will not be so much of a transformation. It will rather be a continuation of the sharing of information by using networks that has been happening for nearly 30 years, since we first ventured into NCW. So before we look to the future, I will just give you a brief history lesson from Navy's perspective.

A long time ago, but well within my memory, all common operating picture information was passed over voice circuits. Then, in the mid-1970s, we upgraded the recently decommissioned *Perth* Class guided missile destroyers with Naval Tactical Data System, known as NTDS. The combat systems from each of the ships upgraded with NTDS could electronically exchange combat system computer information. They did so via a tactical data link which utilised a common standard message format called Link-11. In 1979, the Royal Australian Air Force followed Navy into electronic information exchange when the P-3Cs were fitted with Link-11, and also when the F/A-18s were delivered with Link-4.

So much for history, what are we doing now? All of our major surface combatants are now fitted with Link-11. In addition, the Super Seasprite helicopter, acquired for the RAN under Project Sea 1411 to provide the primary surface warfare strike capability for the *ANZAC* class frigate, will also have a Link-11 capability.

The next generation of tactical data link that Navy is planning to introduce is Link-16. When HMAS *Anzac* deploys to UK waters for Exercise *Northern Trident* 2005, she will have a full Link-16 hardware suite in a stand-alone capacity as she will not have an interface to the Command Management System. Ultimately, Link-16 will bring a significant new capability to each ship in the area of situational awareness. It will provide access to the full Link-16 message set on the network and provide each ship with Combat ID in a coalition Link-16 network.

In order for the ADF to achieve joint and combined tactical interoperability and command and control (C2) functions, it is essential that we have common standard information formats within and across platforms and systems. Data links, such as Link-11 and Link-16, have the ability to exchange information quickly and efficiently between participating units, providing the Joint Operations Commander and subordinate C2 agencies with real and near real-time data on battlespace information. This data necessarily includes the precise location of land, maritime and air platforms—friendly or otherwise—which can be extrapolated to compile a tactical picture, along with information on weapons control and engagement status, intelligence, electronic warfare (EW) and C2 directives.

The benefits of networking sea and air platforms and the use of collaborative tools such as chat rooms were amply demonstrated by Navy's experiences in the Persian Gulf over the past two years. For a considerable portion of that time we commanded the Coalition Maritime Interception Force (MIF), including during the recent

hostilities against Iraq. In broad terms, our use of current NCW techniques gave us a greater shared situational awareness, and also the ability to undertake self-synchronisation. But let me highlight with some examples.

Firstly, in the build-up to the Iraq conflict, the Coalition established a Maritime Interception Operations chat room where the conduct of the MIF was affected. Royal Navy frigates joined the chat room while they were still in the English Channel, and HMAS *Kanimbla* joined the chat room while she was still transiting the Indian Ocean. By the time these ships joined the Maritime Interception Force in the North Arabian Gulf, they had achieved a high degree of situational awareness and, therefore, they were able to achieve an accelerated integration.

Secondly, in enforcing sanctions and conducting mine clearance in the Khor Abd Allah during the war, the units of the Maritime Interception Force and the operational level command headquarters had rapid sharing of the common operating picture, which included selected video streaming. This resulted in vastly improved situational awareness and faster decision-making. Courses of action could be discussed and refined in whisper boxes before orders were posted in the open chat room. The use of chat windows also allowed subordinate units to clarify issues before they became critical. As a consequence, much greater cohesion was achieved within the Maritime Interception Force.

Thirdly, the Maritime Interception Force's increased level of shared awareness through the use of collaborative tools empowered the MIF to be prepared to undertake potentially multiple tasks simultaneously. These nascent NCW capabilities allowed the MIF to self-synchronise when these tasks were required to be executed at short notice.

And lastly, the practical benefit of the seamless transfer of information between dispersed weapons, sensors and command elements was illustrated by another member of the maritime task force, USS *Higgins*. This ship was stationed in the North Arabian Gulf specifically to detect Iraqi missiles for engagement by Patriot batteries ashore. Using her excellent radars and a Patriot data link, *Higgins* was able to detect Iraqi missiles very soon after firing, and immediately cue the nearest Patriot site. This process resulted in Patriot successfully engaging seven of the eleven missiles fired, with the remaining falling harmlessly in the desert as non-threats.

Throughout the combat phase of operations in the Gulf, RAN units continued to enjoy a high level of situational awareness across a widely dispersed geographical area as a result of the shared common operating picture made possible by existing technology. It was this high level of interoperability, practised over many years through the activities such as the *Rimpac* and *Tandem Thrust* series of exercises, that allowed us to join the Coalition in the Persian Gulf seamlessly, and in a very short space of time to be ready for combat operations. Our 12-year history in the Gulf certainly contributed to this high level of interoperability and has allowed us to participate with the USN, the current masters of NCW, as they develop their NCW capability.

But just as our experiences in the Gulf highlighted what is possible through high-level interoperability, they also highlighted where networking gaps exist. For example, chat rooms demonstrated their worth in rapidly disseminating the results from naval

gunfire support missions. Conversely, however, our use of chat rooms slowed the passage of information to multiple recipients when a simple voice sitrep would have sufficed.

A second example is the interoperability problems encountered by Coalition boarding parties and boats. The only way they could have a common encrypted voice communications net was through the provision of 40 Australian Wagtail communications sets. It is hoped that in the future, software definable radios will alleviate some of these interoperability issues. Interestingly, within the ADF, no such problems exist due to the application of common standards across the Services.

What the conflict in Iraq and the Global War on Terrorism have both highlighted to Navy is the need for the enhanced exchange of information between allied and coalition partners. Despite the fact that there have been many different networks established within and between AUSCANNZUKUS and NATO nations over the years, significant issues still remain with respect to establishing and operating secure, tactical coalition wide area networks.

Consequently, Navy has taken a significant role in multinational experimentation regarding the tactical implementation of IP networks. We are a member of the AUSCANNZUKUS Naval C4 Organisation, together with the navies of Canada, New Zealand, the United Kingdom and the United States, which has existed in a number of guises for several decades.

As part of this organisation, since 1997 we have participated in the Joint Warrior Interoperability Demonstration (JWID), which is sponsored by the United States Department of Defense. This participation has specifically addressed the maritime tactical requirement, with the separate national participation focusing more on the joint and combined operational and strategic information requirement.

JWID 04 aimed to demonstrate improved C4 effectiveness and enhanced maritime information exchange with joint and combined forces, through the extension of IP-based networking at sea and in the littoral. It focused on:

- the trial of information transfer between security domains including messaging, chat, common operating picture (COP) distribution and automated replication of web pages between security domains, as well as the use of authentication and non-repudiation;
- the trial of variations of net management with an emphasis on traffic management and prioritisation;
- the demonstration of measures of effectiveness, both operational and technical;
- a limited inquiry into knowledge management and information dissemination management, including metadata availability and definition; and
- the trial of an enhanced situation awareness capability, while spanning multiple information domains.

At the end of JWID 04, all five participating nations agreed on a detailed report, which comprehensively outlines the establishment, execution, conclusions and recommendations arising out of the demonstration. It will be tabled at multinational meetings conducted in Washington in October of this year, and a number of the findings in the report will contribute to the ongoing development of allied navy doctrine in this area.

This sort of leading edge experimentation is sometimes criticised as being ‘big picture’ without delivering tangible outcomes. Navy’s experience has been refreshingly different. JWID Multinational Naval Task Group (MNTG) work has been undertaken in a highly collaborative, cooperative and mutually supportive ‘teaming’ environment, where the five navies have pooled knowledge and resources to investigate real solutions to coalition networking in a low-bandwidth high-latency environment.

From our national perspective, this work has direct bearing upon a number of our projects, particularly Project SEA 1442 – Maritime Communications and Information Management Architecture Modernisation, known as MCIMAMS.

Within the next five years this project will deliver the Maritime Tactical Wide Area picture over a fully IP-based Wide Area Network. In the implementation of this project, Navy aims to convert current stovepiped information services to common IP networks, which will allow the ubiquitous exchange of information between services. This project is an essential element in Navy’s contribution to the NCW Roadmap.

In a similar time frame, Joint Project 2030 – Joint Command Support Environment will in its latter phases deliver the environmental components that will allow the sharing of a common operating picture in the maritime, land and air environments.

Clearly as we move to IP-based networks, bandwidth becomes critical, particularly to our ships with their limited real estate. While, it is widely expected that SATCOM bearers will carry the load, the reality of the increasing bandwidth requirements of all three Services demands other solutions.

Navy through its membership of AUSCANZUKUS has invested in technologies such as Sub-Net relay that will allow tactical IP networking at sea using conventional HF and UHF radio circuits, thereby easing the reliance on SATCOM. This will give us C2 and connection of sensors and shooters in a limited form. This in simple terms is NCW at the tactical level.

It is important to note that in many respects Navy’s investment in NCW through our ongoing engagement of our allies will provide benefit to the other Services. JWID, which now enjoys participation of all three Services, began life as a Naval activity. Navy continues to leverage off the significant development investment of the US Department of Defense through our participation in exercises such as *Talisman Sabre* and *Trident Warrior*, which sees a virtual Australian unit simulated at HMAS *Watson* in Sydney participating in an allied carrier battlegroup at sea.

The lessons we are learning today, and have learned in the past, are being incorporated in the ships of the future, so now I would like to turn to two of Navy's major projects that will be delivering new capability over the next decade or so.

Firstly, Project SEA 4000 – Air Warfare Destroyer Project. The Air Warfare Destroyers (AWDs) will be our primary sea control combatant, and the 'jewel in our crown'. They will contribute to maintaining an assured capability to detect and attack hostile forces and impose substantial constraints on their operations. They will give us the ability to succeed in low-level, high-level, conventional and asymmetric conflicts. They will rectify our perceived area air warfare deficiency by providing a long-range air defence capability for deployed ADF operations. Their sheer size and power and C2 capabilities will give us options that we have not previously had.

They will be flexible enough to change their readiness swiftly between different levels of operations and apply graduated force commensurate with the situation. In a diplomatic role, the powerful presence of an AWD will send a significant psychological message, as well as when deployed in civil law enforcement and coastal surveillance operations. In higher intensity operations, an AWD has global reach with sustainability and controllability, which can be easily withdrawn if required.

The AWDs will integrate seamlessly with the Joint Strike Fighter (JSF), Airborne Early Warning and Control (AEW&C) aircraft, and Ground Based Air Defence (GBAD) to form a complementary package of networked capabilities that will provide a potent ability to gain and maintain air control. These capabilities will be able to provide air defence for an ADF task group operating around Australia or deploying from Australian shores and establishing itself in some other place, either within our immediate region or beyond.

Additionally, the AWDs will be Joint Defence assets able to provide Australia and its coalition partners with a flexible sea control capability, in particular air defence for joint and/or combined operations. They will operate independently, or in cooperation with any combination of maritime, air and land forces, in a multi-dimensional battle space characterised by network centricity, which will link ADF and coalition sensors, engagement systems and decision-makers into an effective and responsive whole.

The first of the AWDs is scheduled for delivery in 2013. However, it is expected that by 2015 the USN will achieve mature and effective Global Information Grid (GIG) capability. After this time, in order for the ADF and, in particular, the AWDs to be able to integrate effectively in high-end coalition operations, we will need an NCW capability on the GIG.

This capability will provide an integrated, scalable, fully distributed processing and transport environment based on commercial technology. It will be able to move information from any source to any destination and it will provide tailored information through intelligent pull. It will be dynamic, adaptive, self-reconfiguring, robust and secure, and will integrate with legacy C4ISR systems. It will permit full exploitation of sensor, weapon and platform capabilities.

The implications of developing the GIG capability will have a profound effect on warfare. It will permit geographic separation and functional integration of command

and targeting, as well as weapons delivery and support functions. The GIG will also provide a single, integrated infrastructure for all military information needs, including C4ISR, fire control and logistics. It will support split base, force projection and information reachback. Most importantly it will provide joint forces with a common situational awareness, a common operating picture, and information necessary for rapid decision-making.

Additionally, the AWDs' operational roles will require the exchange of information via secure voice and data communications. Both voice and data are essential in order to exchange unambiguous orders and surveillance information rapidly with other members of an operating force. A multi-link capability will aid in extending data communications beyond the line of sight limitation of Link-16. The AWDs will have an HF Link-11 path for reachback to higher authority as well as maintaining interoperability with regional partners who do not implement Link-16.

However, we are also looking at the implementation of a more advanced capability such as Cooperative Engagement Capability (CEC). This is a system of hardware and software, which allows the sharing and pooling of fire control-quality radar data on air targets, providing a significant advancement in air and missile defence. This enables the real-time distribution and fusion of sensor measurement data from all CEC-equipped ships, aircraft and land sites, meaning that cooperating units share composite tracks and can function as an integrated air defence net. In doing so, CEC greatly enhances detection, tracking and identification of air targets, expands engagement space, and enables force-wide engagement coordination.

We are all aware of recent Government announcements that the combat system for the AWD will be based on the Aegis combat system. This decision will ensure that the Navy will remain interoperable with the US, the second priority from Minister Hill's announcement on NCW made in May last year. Aegis will come with a modern S-Band radar, which will be able to detect ballistic missiles and this information will be input into the CEC for shared engagement of the targets. The modern S-band Aegis radar has active solid-state planar arrays, a large sensitivity increase, more clutter attenuation features and, just as importantly, wide instantaneous bandwidth. The role of the ADF in ballistic missile defence has yet to be determined and may be as simple as being used for detection only, to the fitting of SM-3 missiles that are capable of shooting down ballistic missiles in a layered defence strategy.

The second project I'd like to speak about is JP 2048, the replacement amphibious capability for HMAS *Kanimbla* and HMAS *Manoora*. This is a multiphase project that will provide the ADF with increased amphibious deployment and sustainment capability to support a land force. One aspect of this improved amphibious capability is the provision of these vessels with a commensurate C4I capability. Our recent experience with the utilisation of the LPA as a command platform has led us to plan for the replacement ships to act as a major NCW node with the equivalent C4 capability to that of the AWDs.

This is particularly important, because of the ability of networked maritime forces, with an embarked land force, to conduct ISR, to convey situational awareness in an emerging crisis, and to allow for a much better understanding of friendly, neutral and enemy capabilities and intentions. This knowledge may help in preventing, containing

or even deterring conflict by signalling national intent without committing to a footprint ashore.

But we must also realistically face the worst-case scenario that we may be required to conduct a non-permissive amphibious landing and subsequently support a land force. In the past, such operations were conducted in a linear manner—that is, we aimed to firstly achieve sea control and then project power.

The high level of battlespace awareness that will be achieved by NCW will optimise and synchronise the activities of forces, leading to enhanced efficiency and tempo for achieving joint effects. Surveillance is a significant component of this awareness and can be considered in the context of broad area and tactical surveillance. Satellite sensors, the Jindalee Over-the-Horizon Radar (OTHR), strategic Uninhabited Aerial Vehicles (UAVs) and Maritime Patrol Aircraft (MPA) will provide networked broad area surveillance. This will be complemented by networked tactical surveillance provided by organic naval helicopters and shipborne UAVs to provide a close-in picture of events.

Additionally, Navy's emerging Rapid Environmental Assessment (REA) capabilities have the potential to be a significant force multiplier, particularly if networked. Much of the ocean areas around our region, and indeed much of Australia's own maritime areas, are poorly surveyed or not surveyed at all. An REA capability that allows an uncharted area to be surveyed quickly and uploaded to an electronic chart in near real-time will give the commander far greater flexibility in manoeuvring his sea-based assets.

REA's enhancement of the RAN's capability to obtain bathymetric data will be of particular value in amphibious warfare in littoral waters. Knowledge of how our systems, weapons and sensors will be affected by the prevailing environmental conditions could be the decisive element leading to a 'go' / 'no go' decision for a contemplated action. The tactical advantage provided to commanders at all levels from the real-time networking of the information provided by REA would be significant. Much of the technology to do this already exists and is a relatively inexpensive investment for a significant return.

These developments will mean that, in the future, we would most likely be able to achieve sea control and project power in parallel to achieve quickly a decisive result.

Evidently, we foresee that the capability that will be provided to the ADF by our new amphibious ships will be immensely useful in any future conflict. With this in mind, we need to articulate carefully the information exchange requirements for amphibious operations in the littoral environment. With these requirements defined, we will be able to establish the C4 architecture for the vessels being replaced under Project JP 2048.

We have not got it all right. Project SEA 1442 has already captured the information exchange requirements for the maritime environment. However, it did not take into account the information exchange requirements for embarked forces and other assets assigned in support of an amphibious operation. Similarly, Headquarters 3rd Brigade has captured the information exchange requirements for land elements, and Chief

Information Officer/Defence has captured the satellite usage requirement for the ADF. However this information has not been fused into a common littoral view, tailored to meet the specific requirements for the conduct of C4 during amphibious operations.

Accordingly, at present a study has been initiated to determine the information exchange requirements of amphibious operations. Once defined, these requirements will be used to inform the C4 architecture for JP 2048 Phase 4, which should be a product of both the maritime and land communications architectures. A common architecture will enable JP 2048 platforms to be able to exchange secure voice and data freely within the joint task force, including other ADF maritime platforms, other ADF units and coalition forces. The sharing of a common architecture will, in turn, advance efforts to deliver improved effectiveness in training and support.

In conclusion, *ADDP–D.3.1 – Enabling Future Warfighting: Network Centric Warfare* states that:

The *Network Centric Warfare* concept is about enhancing our warfighting capability. While not a warfighting concept, it will enable our capacity to fight in the future. It also outlines a conceptual approach to exploring and exploiting the opportunities of *Network Centric Warfare*. The concept is a start point—not the final word.<sup>1</sup>

I am sure that you can see from what I have said today that Navy has moved well beyond a starting point. Our past networking experiences, our in-depth participation in NCW experimentation and demonstration, and our commitment to interoperability with the ADF and our allies, have meant that we are quickly moving forward with many applications and projects to make NCW a reality.

However, the premise behind NCW is that useful information must be provided to people to allow them to make decisions more effectively. The human dimension is fundamental to NCW. Developing the human dimension requires commitment to important issues, such as selection, doctrine, training and education, organisation and enhancing the interfaces between people and knowledge databases. It is only then that we will fully be in a position to reap the rewards that NCW can offer.

Only then will we truly solve Admiral King’s dilemma and understand that which intuitively we know we want more of.

\*\*\*\*\*

## ***DISCUSSION***

*Air Commodore Dennis Green (ADF Warfare Centre):* Sir, in the network centric warfare Navy of the future how do you see the challenges of command and control in a joint force?

---

<sup>1</sup> *ADDP–D.3.1 – Enabling Future Warfighting: Network Centric Warfare*, Defence Publishing Service, Canberra, 2004, p. iii.

*Vice Admiral Ritchie:* I think I've said that right out into the future you would be able to exercise command and control from a greater distance than you can today. Looking to the far future, I think that probably that is somewhere we might like to go. We might like to do the sorts of things that I know people in both the air and land environments would want to do and that is to remove the person from the battlefield, if you like, to put them somewhere safe. The vision that I'm talking about doesn't go that far. I still see command and control being exercised locally, tactically on the spot. I still see it being exercised by Naval people. I still see the requirement for ships that are fitted with the facilities to enable that command and control. I don't have any difficulty with joint command of maritime operations at sea. It's interesting that one of the expeditionary strike groups that is currently in the Persian Gulf—a large collection of sophisticated ships that probably is as big as the Royal Australian Navy—is commanded by a Marine Brigadier General. I'm not advocating that because we don't have any Marines, I suppose. But I think that command and control at sea will be increasingly influenced by headquarters and staffs and people ashore; I don't have too much problem with that.



# THE FUTURE OF THE ARMY AND NETWORK CENTRIC WARFARE

LIEUTENANT GENERAL PETER LEAHY, AO

## INTRODUCTION

Distinguished guests, ladies and gentlemen, thank you for the opportunity to speak at this important event. I am delighted to be able to provide a Land Power perspective to an Air Power Conference.

Nor do I say that flippantly. The Australian Defence Force (ADF) has embarked on the path towards the 'Seamless Force 2020'. That is an ambitious but achievable end-state. The 'Seamless Force' is conceived as being 'beyond joint'. It will be characterised by a degree of collaboration, utilising a common operational picture, and delivering unprecedented simultaneity of effect, that is qualitatively different to anything that has gone before it.

Technology can take us only so far on that axis of advance. Linking sensors and shooters seamlessly is the easy part—developing a truly joint culture and mind-set is more difficult. Our recent experience on operations has been encouraging. The ADF is at the cutting edge of mastery of the rapid decisive effects of the air/land battle. The natural progression is to develop the same proficiency across the operational spectrum, especially in complex contingencies.

## BACKGROUND AND SCOPE

As you will see in the program for this event, I have been asked to speak specifically about the future of Army and Network Centric Warfare (NCW). This subject has been a key Army focus for some years, albeit under different names and across a range of Army concept and capability development organisations. This focus and a need for a coordinated approach to NCW within Army culminated in July last year with the creation of the Directorate of Network Centric Warfare – Army, under the Director General Future Land Warfare – Army.

Since this time, NCW has been integrated into all aspects of Army concept and capability development. It is recognised as a key enabler for Army's *Complex Warfighting* Future Land Operating Concept (FLOC) and has impacted significantly on major Army procurement decisions, such as the Abrams Main Battle Tank and Eurotiger Armed Reconnaissance Helicopter.

However, in line with the aims and theme of this event, I would like to spend the next 30 minutes or so speaking specifically about the future of Army as it pertains to the future of air power. As members of a Defence Force that is striving towards networked operations and increased jointery, the RAN, RAAF and Army are in many respects currently walking parallel development paths. Efforts must therefore be coordinated and each of the Services must look not only to what it can draw from the

others in a joint environment, but also what it can bring to the table in return. Events such as this one are examples of how this coordinated and cooperative development is being implemented within the ADF.

## **COMPLEXITY IN THE LAND ENVIRONMENT**

Army delivers a number of key enablers to the effective application and maintenance of air power within a joint environment that is becoming more and more complex. Complexity in the land environment is the central tenet of Army's Future Land Operating Concept (FLOC) – *Complex Warfighting*. This important concept document explores and analyses the environment and then outlines the Army response and program of adaptation. Importantly, this adaptation program has application to all ADF Land Forces, including those RAAF elements that directly support us. In order to address the topic of the future of Army, I would like to spend the first part of this presentation discussing complexity and complex warfighting.

### **Diversity**

It may seem trite to refer to war as a complex activity. Certainly, it has always been a dangerous, demanding and complicated activity. But we believe that the current degree of complexity in the conflict environment is unique. It has been created by revolutionary technological and political change. This has radically transformed the conflict environment. The threats are diffuse, highly lethal and ambiguous.

In the 20th century, the dominant approach to warfare focused on defeat of the enemy's armed forces. Recent operations have proven that in modern warfare, numerous simultaneous adversaries must be considered and dealt with.

In conflicts from Iraq, Afghanistan, East Timor, Rwanda, Somalia and Cambodia, these adversaries have included guerrillas, partisans, ex-members of defeated regular forces, militia groups, terrorists and organised criminals. But in some form or another, such elements have always existed in areas of conflict.

The level of adversary complexity that Army is shaping itself towards dealing with in the immediate future now also includes drug traffickers, commercial corporations, unarmed protestors and religious groups, looters, people smugglers, hostile media, and computer hackers. All of these are of course considered in conjunction with the recognised principal threat of a transnational terrorist with weapons of mass destruction.

Dealing with this diversity of potential adversaries will be the responsibility of an ADF that, by and large, will remain the regular armed force of a sovereign democratic nation. We will differ significantly from our most likely adversaries with respect to military capability, organisation, defeat thresholds and cultural values. This diversity in operational environment and the principal of asymmetric or mismatched warfare are key elements of complexity in warfare.

## **Diffusion**

In addition to increased diversity, complex warfare sees the diffusion of war across the traditional boundaries with which we have become familiar. The days of the ADF being able to categorise conflict as strategic or tactical, identify areas of the combat zone with fixed boundaries and differentiate between conventional and Special Forces are no longer relevant. While diffusion across these boundaries has always existed to a certain degree, in complex warfighting it has become the norm and requires a flexible and agile approach to the conduct of operations and force composition.

## **Lethality**

The final characteristic of complex warfighting pertains to lethality. Although conventional weapons fielded by regular forces will remain a key consideration in future conflict, equal consideration must now also be given to a vast array of new weapons. Clearly this includes NBC and weapons of mass destruction, but also the less infamous range of weapons, such as eye-damaging lasers, flame and thermobaric based weapons, direct energy weapons, electronic and computer attack, and even car and suicide bombers.

Low cost and ease of construction makes many of these weapons common in modern conflict, while high technology allows others to be easily concealed, transported and operated by individuals. The end result is that land forces already face individuals with the ability to engage targets with extremely high lethality with little to no warning. This has the potential to escalate a conflict quickly or, in the worst case, inflict such unexpected damage and casualties that a conventional force such as the ADF could be strategically defeated in a single tactical instance.

Now if we look at the elements of complexity, diversity, diffusion and lethality that characterise complex warfighting, we have to acknowledge that this is the type of environment we are operating in right now. Indeed, it is arguably the environment we have been operating in for some time. And please note that when I say ‘we’ I am referring to all elements of the ADF that operate in the land environment, rather than just the Army.

## **COMPLEX WARFIGHTING**

### **Overview**

So how do we organise, equip, train and prepare ourselves for successful complex warfighting? We can deduce from the brief overview just provided that the change in environment is fundamental to our understanding of traditional war and conflict. As such, a new philosophy of warfighting is the essential starting point to determining how land forces must fight to win complex wars.

And that is what our *Complex Warfighting* FLOC provides. It is based on the fact that warfare is a fundamental human, societal activity. It is really an extension of politics and is at the most basic level, simply about influencing and controlling people and perceptions. Warfare has enduring features, such as friction, danger and uncertainty,

and these remain extant in complex warfare. What we are seeing is a different manifestation of warfare, rather than a different activity or event.

### **Manifestations of War**

The past manifestations of warfare are the ones we are familiar with and, arguably, are the ones we are currently structured to deal with. These were wars expressed as violent conflict between two or more nation-states where disarming or defeating the enemy's will through battle was the decisive event.

Unfortunately, success in battle in an environment such as this is based on the assumption that the enemy is a rational participant, who can recognise loss and the overwhelming application of military force in order to accept defeat. Clearly, in the case of our most recent conflicts associated with the global war on terror, these assumptions no longer apply. Warfare is now manifesting its enduring characteristics into conflict that uses both violent and non-violent means involving multiple, diverse participants that is fundamentally aimed at the control of populations and perceptions. This is now the decisive event of war. Success on the battlefield is simply one of a number of integrated activities that are a means to an end, rather than an end in itself. Moreover, we face the dilemma of reaping the strategic success from decisive tactical victory.

There is enduring truth to the Clausewitzian classification of war as the violent prosecution of politics. We must never permit our tactical methods to undermine our strategic political end-state. That is why Army believes discrimination is a vital adjunct to precision.

### **Deliverables**

To contribute effectively to winning this manifestation of warfare, Army and the ADF must be able to apply discriminate force as part of a coordinated campaign that applies all elements of Australia's national power. What are the key deliverables of this application of force? What do we need to be able to do in order to contribute effectively? We need:

- the ability to conduct manoeuvre operations against the main military adversary;
- the ability to protect non-combatants and conduct security operations against guerrilla groups and insurgents that are not part of the adversary's regular military forces; and
- the ability to conduct covert and clandestine operations against specific threats, such as terrorism, intelligence services and a range of other elusive and low-profile/high-impact adversaries.

Now it does not require detailed analysis or understanding of the current Army organisation to see that serious improvements are required for Army to be able to operate freely in this manner. Now I say this noting that we have successfully contributed to complex operations since the early 1990s, and continue to do so now. However, this success has been achieved largely through the professional mastery and

flexibility of the officers and soldiers involved, high degrees of cooperation with our major allies, and just in time delivery of essential equipment and specific training. This is not an efficient way of maintaining capability and we need to address a number of areas of weakness in order to maintain our reputation as a world-class Army and to continue to contribute to military operations both regionally and abroad. Addressing these weaknesses is the aim of our current program of improvement known as Hardening and Networking the Army (HNA).

## **THE HARDENED AND NETWORKED ARMY**

### **Overview**

In short, HNA aims to deliver a more versatile Army that is able to execute a broader range of tasks to a higher standard. This is the key element of balance that will allow a hardened Army to change in response to unexpected operational circumstances.

Agility is the next key enabler. It will allow the hardened Army to transition between tasks quickly, smoothly and with better stealth and protection. It is crucial for the development and maintenance of tempo in complex warfighting, and to allow the same force to perform multiple tasks at the same time and the same place.

The final key enabler is orchestration. Orchestrated land forces will be able to synchronise and coordinate effects in order to achieve the discriminating application of force that is central to the current manifestation of warfare. Orchestration occurs within Army through battlegrouping assets into combined arms teams and occurs across the ADF through flexible and interoperable joint and combined interfaces. It is this enabler that resulted in the 'N' in the HNA program as interoperable and reliable C4I systems and network enabled warfighting are fundamental to its realisation.

The key actions of Hardening and Networking the Army also call for the application of new technology and new platforms and it is at this point that I would like to shift specifically to the role NCW will play in the future of Army.

### **Networking the Land Environment**

Army's enabling concept for NCW is based on the premise that networking a force will result in significant enhancements to the synchronisation, speed of command, survivability, responsiveness and overall lethality of the force. All of these things we have already spoken about as crucial to effective complex warfighting. Importantly though, I do not ever see the Army being a network centric force. In all of our doctrine and future Land Operational Concepts, such as *Complex Warfighting*, the commander is central to success on the battlefield. Noting this, it may be more appropriate to say that Army is moving towards network enabled warfare, rather than network centric.

In our efforts to move towards a networked force supporting the commander we have concluded that establishing a single, holistic network in an environment as complex as land is virtually impossible. Even if it were to be achieved, the network and communications overheads would be far too great to manage in a high tempo and complex environment. Our approach is, therefore, to establish a federation of

networks that are seamlessly integrated at designated points within the land C4 architecture. The focus of our efforts is therefore on the interfaces between disparate networks, so that from a user's perspective, there is only one network linking the entire force, providing them with a human-machine interface terminal that is optimised to their specific requirements.

### **Bottom-Up Approach**

The Army approach is also unique in Defence, in that we are adopting a bottom-up approach to networking the land environment. Our immediate focus is on networking combined arms team at Company level and below, with an eye out to networking platforms and organisations from Brigade or minor Joint Task Force Headquarters down. Army has to start at that level because, unlike RAAF and RAN platforms, we currently have no automated means of maintaining situational awareness and no established data links between our combat platforms. It is true to say that, while the RAN is not yet a network enabled or network centric naval force, if Army could achieve the level of combat system integration, sensor-to-shooter connectivity and fleet situational awareness that RAN currently achieves via Link-11, 90 per cent of our NCW goals and objectives would be met.

Due to bandwidth constraints, the number of independent platforms, limited power options and a high mobility requirement, networking at the low tactical level will provide us with the greatest challenges. However, it is here that we will also see the greatest gain from increased integration and situational awareness. While fundamental to complex warfighting, the components of combined arms teams at this level currently have no automated means of battle management. They operate solely on voice communications and synchronise their actions through battle drills, orders and agreed priorities, while at all times maintaining situational awareness through visual contact, manual reporting and hand-drawn map overlays. Understanding this, it should be clear that even a small increase in networked capabilities within the combined arms team has the potential to deliver significant increases in combat power.

The ability of the combined arms team to conduct and win close combat is a key component of complex warfighting. Synchronising the battle management of infantry, armour, offensive support, mobility/counter-mobility assets, combat services support and intelligence will allow land elements to apply overwhelming combat power in a discriminating manner with reduced potential for fratricide incidents. For Army, this is where the focus has to be for realising a hardened and networked Land Force.

### **HOW THE LAND COMPONENT CAN CONTRIBUTE TO AIR POWER**

But the land-based combined arms team does not have sole rights on the application of combat power in a complex environment. Air power, both as an integral member of the offensive support battlespace operating system (BOS) and as a joint asset, brings range, lethality and responsiveness to bear, quickly delivering decisive combat power in support of the land component.

## **Precision and Discrimination**

It is in this delivery of combat power from the air that the land component of a force can contribute the most. In complex warfighting, close combat is critical requiring combat power to be applied in a discriminating manner. I strongly believe that the presence of eyes on the ground with fast and reliable communications to the supporting air assets is the most efficient and effective way of ensuring that the right effect is delivered at the right target at the right time.

The recent incident involving a US aircraft attacking an Iraqi wedding party illustrates this point. To a pilot travelling at high speed, relatively high altitude, with a small visual display and years of training emphasising the need for lightning fast decisions, it is easy to see how rifles being fired upwards from anywhere could result in a hostile response. However, to a trained, well-positioned forward observer (FO) or forward air controller (FAC), such distinctions are much easier to make. The environment allows for better observation, a more considered and less reactive decision, and a more 'human' assessment as to what the threat really is. If in fact the targeted group was a civilian wedding party simply firing in celebration, it is difficult to imagine a scenario where they would have been so catastrophically engaged by a land-based observer.

## **Battlefield ID and Eyes on the Ground**

And this is where it comes down to the human in the loop. While recent advances in targeting, IFF and weapons guidance systems have significantly increased the employment and responsiveness of air assets in close combat, recent conflicts have proven to us that, at least for the immediate future, they are not as sure as a human on the ground. The number of air-to-ground fratricide incidents far outweighs the number of ground-to-ground. This is because ground-to-ground engagement always involves a degree of direct human observation that is not necessarily a part of air-to-ground engagement. Despite the technology applied in land-based combat platforms to aid in target acquisition and identification, the very nature of direct fire weapons requires a human to take a sight picture prior to engaging. Even our long range artillery and missile systems are observed and adjusted by men on the ground watching the fall of shot and confirming their targets through binoculars or direct line of sight.

This disparity exists because combat identification is a two-way street that is only as capable as the least capable system. The IFF system fitted to an aircraft, such as the F/A-18 Hornet, will identify other coalition aircraft as friendly with a high degree of certainty as these aircraft are fitted with interoperable IFF systems of the same capability. As such, we see that air-to-air fratricide incidents are equally as rare as ground-to-ground. The same does not apply to current Australian Army platforms and non-combatants, and it is in the air-to-ground interface that the greatest risk exists.

At this interface, Army is the least capable system in the battlespace. Our elements cannot identify themselves as friendly beyond visual recognition and voice reporting means. These means are often ineffective from the air in close combat situations. ADF air platforms are aware of these limitations and, as you all well know, employ tactics, techniques and procedures to ensure that targets are positively identified as enemy through a number of means prior to being engaged. However, these processes slow down the responsiveness of air assets and, in cases where the necessary degree of

certainty cannot be achieved, limit the application of close air support to land-based combined arms teams.

I see this as an Army problem and we have a vested interest in implementing a technical solution to combat identification in the land environment. We must develop a means by which RAAF and allied aircraft operating in a close air support (CAS) role can automatically identify all Army elements in the battlespace. Army and the Office of the Chief Information Officer (CIO) have already agreed that VMF (Variable Message Format) will be the data link standard employed within the land environment and we look forward to coordinating our VMF implementation with the RAAF, RAN and our major allies to ensure it becomes a means of achieving the seamless interoperability required by a networked force.

Until such time, and perhaps even beyond, I consider the actions of FO and FAC parties to be crucial components of the combined arms team and key enablers to the application of air power. Their role has been proven throughout history. In Vietnam, our Land Forces were able to reach back to US and RAAF delivered fires. This provided a decisive edge on many occasions. The efficacy of this approach was confirmed in the complex environment of Afghanistan during Operation *Anaconda*, when our Special Forces relied on the massive force multiplier provided by air power to inflict heavy casualties on their foe. Indeed, the very survival of the Coalition Special Forces task force depended on timely, accurate and precise provision of close air support. Air power provides certainty and precision to a confusing and blurred operational environment and is absolutely essential when the lives of our personnel and the safety of non-combatants are at stake.

## **THE IMPORTANCE OF AIR POWER TO THE LAND ENVIRONMENT**

Having outlined what I think the Army can contribute to air power, it is probably time to outline what I think the hardened and networked Army will expect in return. The recent conflicts in Afghanistan and primarily Iraq have proven beyond doubt the importance of air power in the success of ground operations. Coalition air supremacy made major contributions to success on the ground via the continual degradation and destruction of Iraqi ground forces, the provision of intelligence, surveillance and reconnaissance data, and by aiding command and control via airborne C2 platforms. Outside of direct support to combat operations, air power provided a high degree of mobility at the tactical, operational and strategic level, and was instrumental in force sustainment through responsive logistics and casualty evacuation.

In short, air power allowed Coalition ground forces to operate with sufficient tempo and combat power to overwhelm the Iraqi forces that simply had no respite from the constant application of deadly fire and rapid manoeuvre.

### **Integrated Offensive Support**

The Iraq conflict was, and remains, a clear case of complex warfare. As such, all of the above is what a hardened and networked Army will expect from the RAAF. We will ensure that our combined arms teams are equipped with the skills, experience and communications equipment required to integrate fully the F/A-18 Hornet and Joint Strike Fighter (JSF) into our offensive support BOS. Key Defence Capability Plan

(DCP) projects, such as JP 2089, AIR 5376, LAND 75 and LAND 125, are already working closely in this area and delivering equipment now that will support real-time information sharing by both voice and data.

### **Strategic Mobility**

Recent operations have also highlighted the fact that Army must be prepared to conduct sustained operations, often outside of our immediate geographic region. In such scenarios, strategic airlift is the quickest means of getting personnel, equipment and supplies into the theatre of operations. This is currently the primary role of the RAAF C-130 fleet and Army is watching closely the future of this capability under AIR 5414.

### **Tactical Mobility and Sustainment**

Once deployed, land forces will look to air power for tactical mobility, up-close logistic support and casualty evacuation. Our Special Forces elements already maintain a high degree of interoperability with Army aviation rotary wing assets, such as Black Hawk and Chinook; however, it is acknowledged that larger deployments of conventional forces will be more reliant on the larger, fixed-wing assets of the RAAF for these roles. Again, the issue here is communications between Army and RAAF elements, and our respective staffs are currently working to address these through projects such as JP 2008 and JP 2072. These projects are scoped to deliver equipment solutions that will allow secure, long-range communications to be maintained between elements on the ground, the aircraft themselves, and also troops and command elements on board the aircraft in airlanding and airborne operations.

### **C2 and Communications Range Extension**

Not taking anything away from these key capabilities, perhaps the most important role for air power in support of the Army of the future is the provision of airborne C2 and communications range extension services. The Australian Army expects to conduct operations across large AOs with relatively small forces. This results in a dispersed force, with great distances often separating commanders from their subordinates. Land-based communications are capable of supporting C2 within concentrations of troops and platforms, but between these concentrations we have become reliant on satellite links as the most reliable means of range extension.

However in large-scale conflicts, the availability of satellite services is far from guaranteed. With a volume of data too great for HF services alone, Army will look towards any airborne platform for range extension of our higher-capacity, line of sight communications systems. This will be a key enabler for establishing the digital communications infrastructure required for a networked battlespace.

Likewise, we will expect our communications and command support systems to be integrated into the C2 suite of dedicated airborne command platforms, such as the AEW&C and to a lesser extent the P-3C Orions. These platforms offer a real solution to the C2 issues of a dispersed land force and provide nodes at which common operational picture traffic from disparate feeds and sources can be collated and broadcast across the battlespace. I do not think I am exaggerating by saying that the

employment of airborne communications retransmission, data collation and command and control will be fundamental to Army's success in complex warfighting and network enabled operations.

## **Space**

The last element of air power I want to discuss before concluding this presentation is space. From a land forces perspective, space is the ultimate high ground and a pervasive medium. Our most recent operational experience has reinforced the growing importance of space-based capabilities in supporting the ADF and this trend will continue into the future. Space assets support command, control and communications, provide intelligence and meteorology, can locate our units and other assets, collect surveillance and reconnaissance data, and are vital for the navigation of ships, aircraft and land forces. In short, space assets already provide us with a wide range of critical operational capabilities and currently there is no effective substitute.

Conversely, it is important to realise that developments in space technology also bring new threats and vulnerabilities. Potential adversaries are enhancing their use of space assets in tandem with Australia and our allies, and we need to counter these emerging threats.

As the ADF's largest user of space, Army has a keen interest in the development of all space-based concepts and capabilities. This is currently not represented by our manning in space-related projects and organisations. RAAF has the clear numbers advantage in this arena and I hope we can address this in the near future. NCW and Concept Development staff from Future Land Warfare Branch have already established close working relationships with the Directorate of Defence Space and space-based projects, such as JP 2008. We have also had direct liaison throughout the last several months with US industry and Defense space agencies, through contacts established at the Defence Space Seminar earlier this year. We will continue to build upon the work already done and Army looks forward to having a shaping and developmental role in the development of space-based capabilities, rather than just being an end user of the services provided. Frankly, it is too important to us not to be intimately involved.

## **CONCLUDING COMMENTS**

It is an undisputed fact that the future of warfighting is joint and complex. The Hardened and Networked Army tenets to succeed in this operational environment are a ready and flexible force that can survive hard hits, hit back harder, and remain adaptable enough to transfer quickly from one type of operation to another. These tenets encompass all of the specific points I have raised here this morning and will see Army transform itself into organisation optimised to take full advantage of air and maritime power. This will happen within the time frame of the current DCP and all three Services need to be on the same path now, rather than parallel ones.

The ADF is already a successful joint force, but we achieve this success primarily through the proficiency, professional mastery and flexibility of our personnel, and this has limitations. We can only make things better through the application of technology,

formalising processes and methods of operation, increased training and exercising, and developing the communications interfaces that underpin a network enabled ADF.

Army is currently investing significant resources and effort into the development of such capabilities and technologies. Our priorities in this field are clear, and interoperability with the RAN and RAAF, based on a compatible digital communications infrastructure, common geospatial information systems (GIS) and an ADF-wide federation of tactical data links is our primary goal. The interfaces between air, sea and land are the key components of a network enabled ADF and I am confident that Army will be positioned to meet its obligations in the development of communications and C2 across the joint battlespace.

But even with the application of such technology, the presence of eyes on the ground and the human interface will remain paramount in the effective application of air power to the land environment. Complex warfighting, close combat and the combined arms team require combat power to be applied in a precise and discriminating manner. This is the realm of FOs and FACs on the ground and is a job that Army can best fulfil.

Air power, including space, is more important to the land component now than it has ever been before. No one will dispute this, certainly from within the Australian Army. However, it needs to be acknowledged that in a joint context, land delivers many of the key enablers to the effective application of air power. Only through fully reciprocated efforts to integrate better our personnel, platforms and organisations will the ADF be able to meet the challenges posed by future manifestations of warfare in a complex operational environment.

\*\*\*\*\*

## ***DISCUSSION***

*Air Commodore Norman Ashworth (RAAF Ret'd):* General, my question relates to the impact of NCW in the future on the individual infantry soldier. How do you think it might impact on his way of fighting? I have in mind just the individual soldier, not his section commander or his leaders up the line.

*Lieutenant General Leahy:* A large part of this issue relates to a project you might have heard of called Project Wundurra, the soldier as a combat system. What we have been attempting to do is to provide a soldier with a suite of command, control and communications plus lethality weapons that mean he would be all-informed. I think we're starting to come to the conclusion that the individual infantry soldier can't carry the power pack required to make all of this work but because of the nature of his environment, which is invariably very lethal, filthy dirty, tiring and very stressful, we don't think we can pump all that stuff into his head. So what we need to be doing is making sure that we filter information down to him and he only gets what is required. We're starting to think that that means he needs to know where he is, he needs to know where the enemy is and he needs to know where his mates are, and that's

probably starting to be enough. He then needs to be able to call for support or fire. Now, I didn't discuss it during the talk on complex war but there's another concept that comes out of this and the fact is we think every soldier has to be a leader. We think that every soldier has to be able to call for fire and be trusted that that fire is going to be used properly. We think that in the very dispersed, diffuse environment that you're not going to be able to rely on having a FO or, perhaps, a FAC there. So we need to make sure that he can get access to fire support but he also needs to have the ability to show that discrimination. The US Marine Corps 'three block war' concept, where one day in three blocks you're doing peacekeeping, humanitarian operations and all-out warfighting. Somehow we've got to get the culture of our soldiers right so that with all this information, the physical stress and all the rest of it, he's still able to think about what he's going to do. We think it's going to be enormously difficult and as we develop through the hardened and networked Army development program there are really three axes. The first one is the equipment and the capabilities; largely, that's being provided by the DCP. The second one is, let's get our organisations and structures right within Army but also externally. And the third one, and I think it's probably the most important but arguably the hardest one to do, is to get our education, training and doctrine right so that we've got people who can be discriminatory and make these sorts of decisions. So, in conclusion, I don't want to fill his head full of stuff that he doesn't need to know, I want him to be able to concentrate on his job.

*Air Marshal Ray Funnell (RAAF Ret'd):* I was very much taken by your point early on, General Leahy, that the ADF is a joint force. It's a comment you made again at the end of your presentation. I think in this area, whether it be network centric warfare or network enabled capabilities, that we view military power in holistic ways. We have to do so if we're to ensure that military power is made available to our political masters in forms that are useful for them to use in the national interest. However, I also see that our doctrinal development is not taking on that holistic aspect and we are advancing along parallel, rather than an integrated path. I was disappointed but not surprised to learn that there's almost no contact between the Air Power Development Centre and its Naval and Army counterparts. I think that is most unfortunate and, particularly in this era of network centric warfare, it's something that just should not be occurring. I fully believe and I've held this belief for a very long time now that we need a 'military power' development centre to aggregate the way in which we think and subsequently use military power. I believe an early start to that would be made by collocating the three separate centres under some overarching organisational arrangement, take them out of the Department of Defence and put them in a location such as Western Creek—I always had that in mind as an appropriate place for it for a whole range of reasons. I just wonder then, General, if you could see yourself, in your time as Chief of Army, being involved in such an arrangement?

*Lieutenant General Leahy:* Thanks for the question Ray. We've discussed this issue a number of times at the Chief of Service level and our current position is that each of us, independently, feel that our Navy Sea Power Centre, our Air Power Development Centre and, in our case, the Land Warfare Studies Centre are important to the single Services and we need to keep that capability much the way that it is. There are some moves depending on infrastructure to collocate, I think at the Defence Force Academy; Army will be staying at Duntroon, which is just over the hill. But I think I'd be representing the other service Chiefs by saying that, yes it would be a great idea

to have a Military Power Study Centre, but we'd like to see someone else do that. We find the people we've got studying our environments are very important to our future and we'll concentrate on that. But I would remark that some of the work being done in the Strategy Group and the development of doctrine, I think, is in fact doing the sorts of things you're talking about—not in the exclusive manner that I know you would like, but it is being done and we are seeing the emergence of, I think, some quite credible joint doctrine which will lead towards the sorts of things you aspire to.



# NETWORK CENTRIC WARFARE AND RAAF PEOPLE – VIGNETTES OF THE FUTURE

**SQUADRON LEADER TIM ANDERSON**  
**SQUADRON LEADER CHERYL NEAL**  
**SQUADRON LEADER DOMINIC SIMS**

## INTRODUCTION

### Why Are We Here?

*(Squadron Leader Sims)*

What will Network Centric Warfare (NCW) mean to us—members of the Royal Australian Air Force as we move into the future? Not in terms of the platforms we work on or support. Not in terms of the systems that we build or with which we interface. What will NCW mean to us? How will we live our lives in this new environment? How will we build relationships and communicate with each other? What will we value in the organisation and, more importantly, what will the organisation value in us? These are big questions and, frankly, the three of us are not here to answer them for you.

*(Squadron Leader Anderson)*

What we hope to do over the next 30 minutes or so is to raise these questions and others—not to provide the answers, but simply to ask the questions. To get in the minds of all who sit here in this place the simple fact that we ignore the human element in NCW at our peril. For over 80 years of the history of our Air Force, our people have always been our greatest asset. It will remain so in the next generation of warfare, the network centric generation. What we hope to bring you here this afternoon is a little bit of human context, and perhaps a little bit of platform a-centric balance.

*(Squadron Leader Neal)*

For each of us, and for those who follow us, NCW will mean different things in different ways for different reasons. We do not claim to have all the answers; we do not claim to know more than you do. What we bring in these concluding stages of this premier forum for the discussion of air power is this: our humble opinions on the impact of the human element in the NCW environment.

### The Challenge

*(Squadron Leader Anderson)*

The challenge in this presentation is not ours alone, we share it with all of you. The challenge is this: how will we maximise our advantage in the battlespace through

realising the potential of our people? How will we ensure that our people are always valued more than the systems and machines that they employ. Why is this so critical? In our opinion it will be the strength and quality of our people that will be the deciding factor, the critical edge, between success and failure in future conflicts. To paraphrase Bill Clinton, 'It's the people, stupid!'.

***(Squadron Leader Neal)***

As we have seen over the last two days, NCW is coming; in fact, much of it is already here. It will be the way of the future. But like all things that are developing, there are considerable uncertainties about what it will look like as it matures and how it will impact on each of us. There is no hard and fast end-state for NCW in the RAAF. NCW will present us all with challenges, barriers and hurdles. But the potential rewards are enormous. Challenges and difficulties have always accompanied the introduction of new things, new ideas and new concepts. As Machiavelli observed, 'nothing is harder to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order of things'. And NCW is indeed a new order of things.

**Who Are We?**

***(Squadron Leader Sims)***

Before we go further, however, we would like to address a simpler, but more pressing question. One that we are sure is leaping pretty much to everyone's mind right about now. Just who are we to be up here talking about NCW and the people of the Royal Australian Air Force?

You have probably read the program, and you have heard the introduction. So you are asking yourselves, 'what could a Ground Defence Officer, an Administration Officer and an Armament Engineer possibly have to offer on this topic?'—particularly in light of the intellectual horsepower that has been applied to the topic over the past two days.

***(Squadron Leader Neal)***

A simple answer for a simple question—people like us, our generation, are going to see NCW mature. We represent a cross-section of the generation of Royal Australian Air Force people that will see NCW move from being a twinkle in the eye of Capability Development to being the norm for how we do business. We realise that we cannot claim to speak for all of our generation, but we are going to give it a go nonetheless.

**Vignettes for Me and You**

***(Squadron Leader Anderson)***

The theme of this presentation is 'Vignettes of the Future', meaning short glimpses of what life will be like in the NCW environment. We were relieved that at least three other speakers also noted that predicting the future is at best problematic. Because, put bluntly, we struggled with developing predictive scenarios—we cannot predict what life will be like in twenty years time, or ten, even five. So, no plays, no skits, no voice

impressions, just our questions and observations that we hope will give you a glimpse of what our collective futures might hold.

Speaking of observations, none of us is aircrew—the traditional operators, the warfighters of the Air Force. In the culture of the Royal Australian Air Force of the past this fact may have doomed our presentation immediately as irrelevant, but we believe that in the Air Force of the future our backgrounds, or anyone else's for that matter, will be unimportant in the scale of things. What *you are* will never be as important as what *you contribute* to the organisation—what you bring to the game!

## **THE HUMAN ELEMENT OF NETWORK CENTRIC WARFARE**

### **What is NCW (again)?**

#### ***(Squadron Leader Sims)***

Speaking of bringing something to the game, just what is the game? Well, if you had not guessed by now, the game is network centric warfare. It is the game of the future, and if you cannot play it well, you certainly will not be playing to win. But what is it? Well, after the past two days if you are still sitting up there in the bleachers and thinking to yourself, 'Yeah, but what is NCW?', you are probably beyond our help or anyone else's.

#### ***(Squadron Leader Anderson)***

Putting it succinctly, and using the words of much more eminent speakers who have gone before us, NCW is a tool; it is a means to enable the operational art—it is a means by which we intend to accelerate our ability to make decisions and act on those decisions. It is the means by which we believe we can ensure decision superiority.

This ability to make rapid, superior decisions has long been recognised as an essential factor in the successful leader—as everybody's favourite proponent of bombing people back to the Stone Age, Giulio Douhet observed, 'Give me commanders with swift intuition'.

#### ***(Squadron Leader Sims)***

This is all well and good, and easy enough to understand. However, there is one thing that we think needs to be emphasised in the whole concept of NCW in the RAAF, and that is the 'W' part of NCW. It stands for 'Warfare'. And our concern is that sometimes the endless repetition of an acronym can conceal some of the true meaning of its parent phrase. We must never forget that NCW is all about warfare. More specifically, it is about winning at warfare, and the human factor is paramount in this. It is people that start wars, it is people that fight wars and, ultimately, it is people that die in wars.

#### ***(Squadron Leader Neal)***

There have been countless books written on the human aspect of warfare. But for us nothing sums it up better than US Marine Corps Doctrinal Publication 1. Simply titled *Warfighting*, it states, '... war is a clash between opposing human wills ... It is the human dimension which infuses war with its intangible moral factors.' It continues,

‘No degree of technological development or scientific calculation will diminish the human dimension in war. Any doctrine which attempts to reduce warfare to ratios of forces, weapons, and equipment neglects the impact of the human will on the conduct of war and is therefore inherently flawed.’

In a nutshell, the human element will remain fundamental in warfare. In the case of the RAAF, it is our people that represent this human element.

### **Three Domains of Warfare**

#### ***(Squadron Leader Sims)***

How the human element fits into warfare, and network centric warfare in particular, can be described by examining warfare in terms of three separate but interactive domains; the physical domain, the information domain and the cognitive domain.

The physical domain represents the physical world in which we exist. It is the place where the situation we want to influence exists. It is where we find the equipment we use and maintain. It is the domain of platforms.

The information domain represents the information and data that our sensors and IT suites manipulate and share. It is the domain via which we communicate and develop links between all the elements of the three domains. In the coming world of NCW, this is the domain of the ones and the zeros.

Finally, and most importantly to us, the cognitive domain. This domain represents the human element. It is a construct of and exists in the minds of people. It is the picture of the battlespace that we build from the information that we receive and interpret. It is where perceptions, beliefs and values reside. It is where decisions are made. It is the domain where many, if not all, conflicts are truly won or lost.

#### ***(Squadron Leader Neal)***

None of this is new. Warfare for thousands of years has been conducted in these three domains. Commanders throughout the ages have always had to worry about the quality of the equipment to be utilised in the physical domain. They have always wanted to know what was on the other side of the hill. And they have always needed to develop an understanding of the situation and make decisions based on that understanding.

### **OODA Loop to Your Hearts’ Content!**

#### ***(Squadron Leader Anderson)***

As you have seen over the last two days, no good discussion on military decision-making would be complete without touching on the OODA loop—a construct with which we are confident that everyone here is familiar.

While the OODA loop construct might be a relatively new invention in the history of warfare, military decision-makers have always, since the earliest conflicts, followed a decision-making process that replicates the process described by Boyd. ‘Observation’,

supported by the gathering of information. ‘Orientation’, the assimilation of this information and the development of an understanding of a situation in the mind of the individual—the development of situational awareness. ‘Decisions’ are then made based on this situational awareness, and ‘Action’ follows.

***(Squadron Leader Sims)***

Decision-makers in the NCW environment will continue this practice, but the future networking of the domains of warfighting will mean that very different levels and types of information will be available to the decision-maker. This represents the ongoing NCW-driven change in the way in which the ‘observe’ portion of the OODA loop occurs. NCW is changing the means by which our decision-makers observe the world. But these observations still must be assimilated into the cognitive domain.

***(Squadron Leader Anderson)***

Unfortunately, or maybe fortunately depending on your point of view, the basic element of the cognitive domain, the human mind, remains unchanged. And it is the human mind that orients information, develops situational awareness and, based on that knowledge, makes decisions on courses of action. Networking the domains of conflict ensures that the ‘observe’ portion of the OODA loop can be accelerated and improved. But improvements to match this acceleration in the ‘orientation’ and ‘decision’ steps—the steps of the loop that occur in the cognitive domain—will require improvements in the way we train our people to think. It will require a paradigm shift in how we develop proficiency in the cognitive domain.

**Proficiency in the Cognitive Domain**

***(Squadron Leader Neal)***

In simple terms—in terms which will relate directly to our ability to operate successfully in the NCW environment—proficiency in the cognitive domain boils down to fairly basic constructs. It means being able to assimilate information rapidly and being able to contextualise appropriately that information in order to create superior situational awareness. Finally, being able to make timely and appropriate decisions based on that knowledge. How do we ensure that our people are capable of achieving this—of being proficient in the cognitive domain?

***(Squadron Leader Anderson)***

Firstly, we must understand how people assimilate and contextualise information and how this ‘knowledge’ then informs their decision-making process. What are the factors that influence how people take raw, observed information, and turn it into knowledge and understanding in the cognitive domain? A common analogy in many writings on NCW is that people interpret information via a lens, a filter, of our individual understanding of the world.

***(Squadron Leader Neal)***

This lens is shaped and coloured by numerous factors, not the least of which are our upbringing, our perception of right and wrong, our personal experiences, our training, our values and the culture in which we work and live. Every piece of information that enters the cognitive domain passes through this lens—nothing escapes. But rather

than being a barrier or a hurdle to proficiency in the cognitive domain, this lens offers us the most obvious opportunity with which to prepare our people for success in the NCW-enabled Air Force. It is this development of the minds of our people that will ensure that we maximise our realisation of the potential that NCW offers us.

## **ENABLING OUR PEOPLE**

### **Who are They Anyway?**

#### ***(Squadron Leader Sims)***

In essence, what we are saying is that our personal experience, training, values and culture affect the lens which supports a person's 'orientation' and 'decision-making' ability—the fundamental aspect of superior performance in the accelerated information environment of NCW. Is there a special type of person out there designed for network centric proficiency? Are we going to pursue a new type of super recruit? Is there something wrong with our people now or with our present culture? What training can enable someone to make better, faster decisions? These are all obvious questions to ask.

#### ***(Squadron Leader Neal)***

Perhaps we should start with a look at who our people are likely to be in future. This will directly influence how we train people for proficiency and success in the NCW environment. A number of US Department of Defense reports stipulate that NCW will require IT specialists to perform in the NCW environment. We probably will need a number of IT specialists to support highly technical systems, but in all honesty, NCW is about systems that support people, not the other way around. What we will need are people who are comfortable interfacing with information technology. Essentially, what any teenager today takes for granted. They might not know how the technology works, but they know how to make it work.

#### ***(Squadron Leader Anderson)***

If we assume that this level of familiarity with IT will exist across the population, what then really distinguishes those we recruit today from those we will recruit tomorrow? Simply put, nothing. Who we will want tomorrow is exactly who we want today—high achievers, judged against societal norms. We note that, based on statistical predictions of demographics, recruiting such people will become increasingly difficult. While overcoming demographic constraints is outside our bailiwick for today, we do note that any force development options for the future Air Force will need to address this. But we say it again: who we want is still going to be the same.

#### ***(Squadron Leader Sims)***

The future target of Air Force recruiting will not necessarily be just school-leavers, however—future Air Force members may have been laterally recruited from other Services or industries. There will be more women, and we may have an older force. They will bring with them a broad range of experiences. But they will still be the same sorts of people we recruit today—us. And like today, there are some things that

we cannot influence or change about our people—essentially, those aspects of who they are when they come to us.

### **Help Me to Learn – Help Me to Help Myself!**

#### ***(Squadron Leader Anderson)***

It begs the question, how will we take this diverse group of people and prepare them all to succeed in the NCW Air Force of the future? We will do this in much the same way as we approach it today. We can shape aspects of the lens through which they perceive and, therefore, shape their perception and understanding of the environment—and of the battlespace. It is via the impact of training, and education and the influence of organisational culture that we will make ready our workforce for NCW.

We are not here to discuss in detail all the different aspects of training. Training is important—training is about learning to fire a rifle, turn a spanner, or fly an aircraft. We will continue to require these sorts of basic military and specialist training skills for our day-to-day tactical jobs, particularly at the junior levels.

#### ***(Squadron Leader Sims)***

But as the Chief of Air Force has already identified, we need to have ongoing learning and education processes to develop all of our people—learning and education, as opposed to simple training. We need to develop a values-based flexibility of the mind, as opposed to instinctive or rules-based reaction, to maximise the potential of NCW. Learning and knowledge allow us to contextualise and deal with individual and new circumstances as they arise. This supports superior cognitive performance and situational awareness. Training is important, but education and learning create adaptable minds capable of rapid orientation and decision-making—NCW-enabled minds.

#### ***(Squadron Leader Neal)***

A little story to illustrate the point. In 1990 the then Personnel Manager of IBM Australia, a member of one of the largest and most successful IT companies in the world, said this, ‘IBM ... is looking for first-class thinkers who can be taught on the job what they need to know about computers’. He continued, ‘with today’s pace of innovation, technological change and growth of knowledge, the content of what a person studies becomes less important than their demonstrated ability to learn and think clearly’.

#### ***(Squadron Leader Sims)***

Does this not apply just as succinctly to our own organisation? The way in which we develop our people must encourage a love of learning, understanding and knowledge. It must be an ongoing process—not limited to training courses. And it must carry on throughout an individual’s career. Through education we help our people to help themselves. Learning is the responsibility of the organisation, its leaders at every level, and the individual. People will need to have the broadest possible education, which incorporates an understanding of the roles and responsibilities of others within our organisation, as well as the environments and cultures within which we work.

They will need the broadest possible knowledge base to assist with contextualising information.

***(Squadron Leader Neal)***

We have already said that people of tomorrow will essentially be the same as those of today, with quantifiably similar intellectual capabilities—they will be issued with the same brain; their synapses will not fire any faster than ours. In order to maximise individual potential we have to re-evaluate how we educate people—it is about learning to think in a completely different way. Learning must be a continual and ongoing process aimed at maximising proficiency in the cognitive domain. This can only be done in an environment supportive of learning.

We are already beginning to consider how we will approach and develop this through initiatives like ‘Air Force Learning 2020’. The real challenge will be turning concepts into organisational reality. The ability to pursue actively these sorts of challenges will need to be continually reinforced through our organisational culture.

## **NURTURING THE ENVIRONMENT**

### **Building the right culture**

***(Squadron Leader Anderson)***

We have spoken about how we will help develop our people into proficient and NCW-enabled individuals. What about the environment that we create for them to do their jobs? What about the culture that we encourage to allow these minds to grow and be successful? Culture is spoken about often these days. Culture is about how we do business—it is not necessarily what we say, it is a very obvious set of behaviours that define who we are and how we operate.

Our doctrine says that ‘NCW *assumes* that the force is highly professional, well organised, and has excellent training and leadership’. This doctrine should perhaps have said, ‘NCW *requires* that our force is highly professional, well organised, and has excellent training and leadership’. We must make sure that our culture supports the development of these characteristics and never takes them for granted.

***(Squadron Leader Sims)***

To achieve this, we will need to be progressive and open; we will need to encourage new ideas, new ways of doing things, to nurture innovation. In the past, our culture has not always met our needs in these areas. We have been guilty of tribalism and reactionism, risk aversion and rules-based decision-making.

### **Towards a Progressive and Open Culture – Eliminating Tribalism**

We would argue that chief amongst these in terms of its destructive power is tribalism. Within our Air Force, we have seen tribalism between specialisations; across Defence we have seen tribalism across Services and provider groups. Tribalism is an anathema to NCW. It encourages the hoarding of skill sets and, more damagingly, the hoarding of information. It encourages stovepiping of employment

sets and drives a wedge between specialisations. It clings to a preconceived worth of the value of other people's knowledge, skills and value to the Air Force.

***(Squadron Leader Anderson)***

A conservative, platform-centric air force, embracing tribalism, denies itself an enormous portion of its cognitive potential. The most obvious, and well-worn, example of this is the entrenched concept that only pilots can lead our Air Force in its key positions. This may have suited the Air Force of the past, but what of the future? At what point does clinging to this concept as a cultural standard become tribalism, and by its very nature obstruct the open culture we are trying to build. This is not an example that we throw in lightly, given both the audience here, and the fact that for all three of us our entire command chains all the way up to the Chief of Air Force are both here, and are aircrew. Nevertheless, in the NCW environment initial specialist training need have only a limited influence on your future—either in terms of being a successful leader, in management or in operations. If our Air Force is to perform to its maximum potential, we must ensure that the right people are identified and developed to perform in the cognitive domain, regardless of their initial specialist training.

***(Squadron Leader Neal)***

Think about it! Conceptualise the wasted intellectual and leadership resource passed up in the last 80 years due to the cultural belief that only a small percentage of the organisation—originally selected for their suitability for initial specialist training—has the necessary skills and cognitive ability to progress to its highest levels, be it strategically, operationally or in the human resource management sector. It is an old argument, and one that we do not want to labour over, but it serves as a stark reminder of how tribalism can limit the potential of our organisation.

***(Squadron Leader Anderson)***

In the network centric environment of the future our adversaries will be doing everything to outmanoeuvre us in the cognitive domain. We must ensure that we make best use of all of the intellectual and cognitive potential of our Air Force to overcome our adversary. It may be that the shape and nature of our specialisations will have to change to allow us to push forward those who are best suited to operate in the NCW environment—and we do not just mean officers, we need to do this across the organisation. Our personnel systems must be designed to ensure that those who perform to the highest levels in the cognitive domain are identified and developed to maximise our advantage in the NCW environment. It is about building a winning culture—it is about minds, not specialisations; merit and capability, not criteria.

***(Squadron Leader Neal)***

In the NCW environment our Air Force requires the best possible people at the right place at the right time. The best people are those who assimilate information the fastest and the best. That is, they have demonstrated the ability to perform in the cognitive domain.

## **Towards an Effects-Based Organisation**

We must continue to evolve as an organisation. How we view ourselves must change. We hear a lot about effects-based operations. What we also need to work on is creating an effects-based organisation. An organisation that has a very clear understanding of the effect it must achieve, and then reverse-engineers its organisation and structure to meet this end-state. Conservatism and reactionism that hold onto the current views and ways of doing things will hold us back.

### ***(Squadron Leader Sims)***

Clinging to misguided and nostalgic views of individual specialisations' historic value to the organisation will only limit our ability to innovate, and will prevent the creation of the right environment to maximise the benefits of NCW. This is something that we already recognise. For example, in response to concern about comments on the future demise of the navigator specialisation, our Chief of Air Force wrote, 'naturally, as the Air Force transitions to the future and we bring into service the new generation of platforms across the combat spectrum, the roles and responsibilities of many current specialisations and trades will also transition to meet the new demands. I see the function of 'navigator' falling into this category ... Our future Air Force will rely on a range of highly skilled people, working together, and across a variety of disciplines, to meet the unique, and new, challenges that we will inevitably face.' That our Chief had to make this point so publicly perhaps points to the fact that we are not quite ready to let go of our past.

### ***(Squadron Leader Neal)***

We have a responsibility to embrace the evolution of our Air Force to an Air Force better suited for NCW—regardless of what we do now. It is hard for all of us, as we are naturally resistant to change. Our culture must encourage us to adapt to new environments and circumstances. It must encourage us to innovate.

## **Innovation – The Elimination of Risk Aversion and Conservatism**

Innovation can occur at many different levels—operationally, in developing courses of action; organisationally, in terms of experimentation and capability improvement; and individually, in terms of maximising productivity. Encouraging innovation across all levels will fuel new and effective ways to develop and project air power. This will give us an edge over an adversary—which we should never forget is the whole point of NCW.

### ***(Squadron Leader Anderson)***

Innovation will allow us to drive change in our environment, rather than having us react to a changing environment. Our culture must drive us to innovate, rather than react. We must remain open to new ideas and not simply discard them because these ideas do not sit well with our current doctrine. Doctrine is wise guidance—as Group Captain Finn said, 'it explains and informs'—it is not dogma. Our people must be encouraged to understand that innovation is a fundamental process in our daily business. In fact, we should place a high value on our people who see things others do not. We need to support these people and reward and motivate them.

***(Squadron Leader Sims)***

Certainly, we must all understand that success in innovation is not always guaranteed. Nonetheless, the culture of our Air Force must encourage trying new things and making mistakes—because this is from where true innovation comes. It must also support open and frank discussion of mistakes and lessons learnt.

Supporting this must be an understanding that punishment does not follow failure—learning follows failure. As Henry Ford said, ‘One who fears failure limits his activities. Failure is only the opportunity more intelligently to begin again.’ It is about reaching beyond the known and finding new ways of thinking and operating—about gaining a warfighting edge. It is about engaging the adversary in the battlespace of *our* choosing.

***(Squadron Leader Anderson)***

In the past, perhaps, we have not always created an environment where innovation flourished. Ask yourselves these questions, honestly. How have we reacted to mistakes in the past? How have we viewed people who have tried to challenge the status quo? Is not making a mistake in front of your contemporaries considered to be a career-limiting move? The problem is that people, who are made to be defensive about mistakes because they are attacked for them, cover up problems and start looking to place blame. In the end, everyone becomes so busy denying mistakes that they cannot learn from them.

Innovation is a focused effort to introduce new ideas and new ways of doing business—and this involves risk. Our culture must understand that with innovation comes the risk of failure. Our culture cannot support risk aversion. People must not be afraid of trying new things for fear of being punished as a result of potential failure—rather, failure must be seen as a learning experience that will support future successful innovations. It will take leadership at every level to see this achieved.

**Flexible and open leadership**

***(Squadron Leader Neal)***

We cannot underestimate the importance of leadership in the NCW-driven battlespace. Even though we may expect that hierarchies will flatten and our workforce may become more geographically spread out, leadership, at every level, will continue to be the mortar that holds our Service together. It will also be a key driver in operational success. Leaders must be able to understand the context of operations and provide clear and concise commander’s intent—this is critical to NCW. They must also be prepared to delegate the authority for decision-making to the lowest appropriate level. They must trust their subordinates, to whom they have given all the tools necessary, to get on and do the job. NCW brings the battlespace closer to the higher level commander than it has ever been. RAAF leaders of the future, despite this proximity, must avoid the temptation of reaching down, and must maintain focus on *their* level of responsibility.

***(Squadron Leader Sims)***

Now, as in the future, our leaders must lead by example. In particular, they will be required to be values-based in their behaviour—because nothing is so destructive on a progressive and innovative culture than rules-based and inflexible micro-management. If we want more experimentation, learning and innovation in the Air Force, we must establish a culture that builds self-confidence and trust in our people.

**Trust Me!**

You see, NCW is all about trust—it fuels the whole network centric concept— trust between specialisations, trust between Services; essentially trust between our people. Trust is extraordinarily fragile and building it is a subtle, long-term process. It does not come from what we say—trust is built or destroyed by what we do.

***(Squadron Leader Neal)***

The Chief of Air Force said it yesterday in his opening address: ‘the key to NCW is the relationships engendered by people’. What we have just described to you in terms of cultural adaptation—in eliminating tribalism and encouraging innovation—is all built on the cornerstone of personal understanding, relationships and trust:

‘I trust you for what you contribute, regardless of who you are.’

‘I trust the information that you provide me, and I trust that you will believe mine.’

‘I trust you to try new things, to innovate.’

‘I trust you not to punish me for making mistakes.’

‘I trust you to make decisions.’

***(Squadron Leader Neal)***

We need to share information across all areas of the organisation. We need to value all information on its merits to develop the best situational awareness. Pre-valuation of information within the network will undermine the acuity of that information. Every node in the net must trust every other node—people must trust people. Whenever we retreat into our stovepipes, we undermine relationships and trust. We must ensure that from the very beginning of every Service career that a key tenet of education is learning to trust and to build relationships.

**WHEN ALL IS SAID AND DONE**

**Ours is the Future!**

***(Squadron Leader Sims)***

There it is. Remember, we never said we were going to provide you with all of the answers. Have we been overly general in our discussion—yes! Why? The three of us do not have an exclusive ownership of the future. We have undertaken only to offer

you our observations on where we think we need to go. Where we actually go will depend on the leadership that guides and directs us and, more importantly, on our shared vision and understanding of our future. We hope that by giving you our observations that you will have had a glimpse of what your vignette of the future might be.

***(Squadron Leader Neal)***

Things must change. This is not a criticism; in fact, it is a challenge. We would never propose that we have to abandon who we are and where we have come from. Ours is a rich history of service and sacrifice. It stands both as a solid foundation for what we do and as a reminder of who we are. We are the people of the Royal Australian Air Force—but in the same breath, ours is the future!

The world, and with it warfare, is a changing, evolving place. We have the opportunity to ensure that future generations of our Air Force are able to maximise the potential of the network centric environment. That opportunity will be realised through our people. We must seek *now* to bring to reality all that we have spoken about.

**The Future – An Undiscovered Country?**

***(Squadron Leader Sims)***

Air Force people of the future should expect that the truly NCW-enabled air force of the future will understand that success in the cognitive domain is an essential aspect of Air Force operations, and that this will only occur through an organisational culture that sees innovation as the norm, that actively pursues the ongoing education of its people and recognises the contributions of all of its people. Ultimately, we should all expect to work in an Air Force that seeks to achieve through its people a better, more efficient and more successful way of operating across the spectrum of conflict.

***(Squadron Leader Anderson)***

And we are not really that far away. These concepts do not lie in some undiscovered country. We have already established the ‘Adaptive Culture Program’, aimed at encouraging an open and progressive culture. Our ‘Leading Edge Teams’ have been created to drive innovation across the organisation by utilising the brain power of our bright, young people. ‘Air Force Learning 2020’ will bring new ways of training and educating.

NCW is created by people for people—it is there to help us in achieving the ongoing security of our nation and its interests. Whilst platforms and information will always be there to support us in achieving our strategic, operational and tactical objectives, we must never forget that it is through our *people*, through their success operating in the cognitive domain, that all our future conflicts will be won.

And in the end, is not this what NCW is really all about?

\*\*\*\*\*

## **DISCUSSION**

*Major Michael Leichsenring (Army – Ground Liaison Officer No 2 Squadron):* In his presentation, Dr Alan Stephens said, ‘How can people network if they don’t talk to each other?’. I ask the panel to offer their humble, cognitive opinion on the requirement for Liaison Officers. Will network centric warfare require them, or do away with them?

*Squadron Leader Sims:* I’ll leap forward on this one. A Liaison Officer, in my mind, is someone you need when you’ve identified that you’ve got a cultural difference and you need to go and find out about a different organisation. Yes, Liaison Officers will be required in the short term; they’re a fabulous way actually to start bridging the gap between cultures. In a truly NCW enabled ADF, I’d like to think that Liaison Officers weren’t necessary because, as we would hope, everyone would have a broad understanding of everyone in the organisation—they understand how people work, who they are and what they can do for them.

*Squadron Leader Anderson:* If I can just take that one step further. If what we’re talking about here in Air Force, about identifying the right people and moving them up through the organisation, is expanded to a joint proposition, that’s where I think you do get truly beyond joint; where everybody in the organisation, regardless of what Service they’re in—for Air Force, we say regardless of what specialisation—regardless of what provider group you work in, if you have the right stuff, then as you’re moved up through the organisation you get the necessary skills that you need and at the end of the day it really does not matter what ‘tribe’ you’re from, you’re simply a contributor to the effect.

*Squadron Leader Philip Gordon (RAAF – Australian Defence College):* Thanks very much for the presentation. You started your presentation by quoting US Marine Corps doctrine that said warfare is not a science, and yet the slant of your presentation was on an intellectual capacity for the decision-making abilities of the future. I did not hear you mention the warrior ethos or fighting spirit at all. I put it to you then that the fighting spirit is as important as intellectual capability to winning the war and is probably what has resulted in Australia being so successful in the past. Do you have any comment to make on this?

*Squadron Leader Anderson:* To be honest we could have talked for another hour and a half but everybody would have missed their planes home. But yes, you’re right, it is just as important. There are so many things we would have liked to have covered. We would have liked to talk about the culture of the people coming into our Air Force and how it might be different from now. We would have liked to have talked more about the individual operating in the battlespace. But, we said it before and Dom [Squadron Leader Sims] concluded by saying, it’s not just up to us—the three of us sitting here answering your questions. I’m sure that many of you could answer your own questions in that way; about how you feel about the culture that you work in and about how you’re going to go about making the culture better so that it suits your vision of the future, which is a real motherhood way of getting out of answering the question, but at the end of the day there it is.

# **OBSERVATIONS ON THE CONFERENCE**

## **AIR VICE-MARSHAL ROXLEY MCLENNAN, AM**

Air Chiefs, distinguished guests, ladies and gentlemen, it is surprising how often I take a stage following Air Force youth and suddenly get confronted with my own feelings of inadequacy and threat, I suppose, when faced with such quality. But I guess that is one thing I really enjoy about the Air Force when I look around it and see the quality of people coming ahead and get such confidence in the future of our Air Force when I realise that this is the next generation and that there are even better generations following after that. I have been afforded the privilege of making some brief observations on the conference, and they will be brief because I am cognisant of the fact that we are already running just a little bit behind time.

We have been treated to a very interesting conference from a wide range of speakers with very diverse views, focused on the network centric warfare theme within the future of air power but, nevertheless, identifying a significant number of challenges in the way ahead. For me—and this is personal observation; I could be taken to task on any of this—the recurring themes throughout the days have been people, jointery and extending that jointery into interoperability or combined operations, technology and time. When I talk about time, I mean time in the broadest sense of the dimension: tempo, complexity, decision cycles, development and acquisition cycles, and all the things that go with it. I cannot touch on everybody's speech in the depth that I would like to and I need to apologise that they will not be receiving due justice, because I have got less than a minute on each presentation and you simply cannot do justice to the quality of the presentations, the depth of thought that went into them and the expertise that lay behind them. Therefore, I am only going to be able to offer the briefest oversight of where we have been and how they contributed in each and every case to those themes that I have identified. Now, the themes of people, jointery, technology and time, I did not put them down in any specific order but I think I would be prepared to take on an argument at any stage but that is probably the priority order in which they should stand.

We started with the opening address by our Minister for Defence, Senator the Honourable Robert Hill, who spoke on 'NCW – The ADF Roadmap'. He noted that we must be prepared for a wide range of contingencies at short notice; therefore, we need a broad suite of capabilities. He talked about rapid prototyping and development, and a program between Defence and industry, he touched on the JSF and noted that information superiority is the most critical element for success. He got all of those themes within that area. He also made a couple of quiet political announcements, which was good, but I think the important element of his presentation was the fact that he was here and demonstrated the relevance of NCW at the very highest level, that is at the Government level. That was followed by Air Marshal Angus Houston's Keynote Address, 'The Future of Air Power – RAAF Response to the ADF Roadmap'. He identified, up-front and as the highest priority, that key element, that key theme of people, noting that networking is about relationships that enable superior decision-making. He noted that people are the key to NCW and our future generally, and he noted the importance of the right people, values based culture—and it's all

about culture—and leadership. He also noted that a strategic uncertainty pervades, so we need a balanced force but it must include the high-end warfighting capabilities. The force must, of course, be expeditionary and it must be tailored, flexible and networked. It needs to be pro-active in working towards the networked future. To end the first session, we were addressed by Lieutenant General Joseph Hurd, who spoke on ‘Network Centric Warfare and Air Power’ and entreated us to keep NCW in perspective. He noted that it is not a new warfare doctrine, but it is an enabler. And technology is not the hardest part but rather, getting back to the people again, it is the culture that needs to change. We need networking interoperability, we need standards, architecture and language, we need the framework but, once again, the central point of his presentation I believe was really all about people and it was all about culture.

Air Vice-Marshal Iain McNicoll from the Royal Air Force, talking on ‘NCW – Perspectives from the United Kingdom’, drew a distinction between Network Enabled Capability (NEC) and NCW, that the network should be our servant and not our master, and that we need to function within the NCW concept beyond just the warfare itself. His recurring theme was command and control. Once again, we get back to the really central and important element of it. Amongst all the technology, all the timeliness and so forth, again it is about people. He talked also about the reduction of the number of platforms to allow networking; in other words, the synergy associated with the technology and the ability to network, which means that you can do more with less because of the synergies that you develop out of that.

Then we had the international panel; the theme of that was ‘The Value of NCW to Air Power’. The first panel speaker was Air Marshal Subhash Bhojwani from the Indian Air Force, who spoke of the advantage of starting network centric warfare late. If you are a little bit late, you get a more mature implementation. Certainly, that applies in Australia’s case; we hope we are just not too far behind. He talked about the legacy platform options and what you might be able to do with them: selective upgrading, early retirement. There are some very significant strategic decisions that need to be made there and, indeed, those are the decisions that Australia is grappling with at this very moment. He also noted that NCW encourages counter network warfare and then counter-counter network warfare. I understand—I do not know whether it was light-hearted or not, Subhash—that you declared counter acronym warfare on the USA. You will need to note that, as an ally of the USA, we have standing by at short notice readiness to move some counter-counter acronym warfare experts in the Department of Defence. They are mostly Army and in the Public Service but, nevertheless, they are very capable. Lieutenant General Dato’ Azizan bin Ariffin from the Royal Malaysian Air Force followed. I understood his greatest challenge was being on just after lunch and speaking on a subject that some experts had previously addressed. Nevertheless, he came through, noting the great challenge for small air forces is the resources and the confusion due to the changing nature of NCW. The point about it all is that we cannot benchmark on the standard that the US sets. We can follow, we can coordinate and we can be part of that but a lot of countries, Australian included, need a more modest approach, a realistic approach. But what network centric warfare does is it increases your allies because of the interoperability that it induces into your force structure and your future planning. We do need to sharpen the back-end functions, that is logistics and intelligence, before the networking. In other words, we have to have our fundamental systems in place before we take that step of networking, which

will only serve to confuse if we don't have the basic structure tidied up and ready to play.

In the last session yesterday, Professor Ross Babbage from Strategy International talked about 'NCW and the ADF – Criticisms and Potential Pitfalls'. It is unusual to hear Ross give a negative approach to anything. Normally, he produces solutions and ways ahead. But he did create some very interesting thought processes when he identified 12 major criticisms of NCW and posed the question, have we got them all covered? He noted that training is a major recurring theme in addressing the criticisms. He noted our vulnerability to psychological attack, which will undermine confidence in the network, and he noted that NCW without an effects-based strategy may well be to no avail. Picking up the theme from the first presenter, he highlighted that NCW is just a tool; it is not an end in itself.

Dr Alan Vick from Rand Corporation talked on 'Seven Propositions About Close Air Attack on the Future Battlefield', noting that air power is increasingly lethal against ground forces. He suggested that in addition to air control we can now do land control down to brigade size. Is this a new growth role? The adversary will not try massed land forces, so friendly land forces may be surprised and it increases the need for responsive air attack. Once again, he developed this joint theme. He also introduced the element of timeliness associated with the network environment. Dr Alan Stephens, speaking on the history of NCW, started with a rather new perspective but he did pick up on that first fundamental and important theme of people. He noted that NCW is not new—it started in World War I with some hand signals—and actually it is all about the cultural difference between airmen and soldiers, and interpersonal communications are critical. Sanu Kainikara followed on with a paper on 'Future Options for Australian Air Power' and led us from the historical perspective effectively into the future and noted the serious challenges to conventional air power, nano-technology among others.

Then we were treated to a very comprehensive, but very succinct, high technology picture of the future from Lieutenant General Carl O'Berry from Boeing, who talked on 'Network Centric Operations and Modular Systems'. In particular, he highlighted that we need to use all the appropriate systems as communications nodes. He focused also on the acquisition side of the house. Time again featured very importantly within his technologically based presentation and with particular relevance to Australia, the Kinnaird Review<sup>1</sup>, which is a recent review that has changed the way we do the acquisition business, in some respects perhaps is a little bit at odds to the environment that we are now moving into, in that technology is changing so quickly that the process—a very good process of acquisition capability development but one that takes a significant amount of time and is very detailed—may, in fact, be self-defeating if we achieve the acquisition of technology which by definition is already out of date before we get it. Group Captain Chris Finn provided us a very good insight into the doctrinal issues associated with NCW. He noted, in particular, that doctrinal issues or roles are valid and enduring, but the relationship between NCW and effects is difficult to grasp as a concept and it is going to be critical that we get our minds around that. Air Vice-Marshal Julie Hammer, Chief Information Officer, talked about information

---

<sup>1</sup> *Defence Procurement Review 2003*, an external review of Defence acquisition and management, initiated by the Government to identify improvements in Defence project management. The review team, led by Mr Malcolm Kinnaird, submitted its report in August 2003.

management and the way the Australian Department of Defence does it as the key to NCW. Specifically, she noted that we need to manage information as a capability, and that I think reinforced what had already been presented by Carl O'Berry. She highlighted that Defence manages, arguably, the largest information environment in Australia and that we need to develop a robust information architecture framework to manage that. In other words, we need a proper map so that we can see where we are going before we embark upon the journey.

I will group, if I may, Vice Admiral Chris Ritchie (Chief of Navy) and Lieutenant General Peter Leahy (Chief of Army) because, while they spoke on very different themes, they spoke from a 'tribal' point of view. Their fundamental point was consistent and that fundamental point focused on the people, the jointery and, of course, the technology associated with facilitating that. What I certainly got out of those presentations was that the networking that we are now developing and moving towards is going to drive jointness, whether we like it or not, and the two are inextricably linked. Then, finally, we really got to the heart of the matter, which is people, and I do not think I need to say any more about that last presentation. I am not even going to think about commenting on whether an ADMINO [Administration Officer] might lead the Air Force, but Chief of Air Force may wish to do so.

We did have, over the course of the two days, several points of divergence and a lot of those points of divergence I have to say came from our overseas speakers, which is fundamental to the enriching nature of a conference such as this. So I thank you for those divergent views but, at the end of the day, I think a lot of those divergent views actually came together to support a fundamental understanding of the challenges that face us and the difficulty we are going to have in addressing them. Certainly, one of the points of agreement was that network centric warfare is not an end in itself; we need to consider effect. Also, it does need considerable technological support and, most importantly, effective communications. But it is not just about technology; the main challenge really is human. It is particularly associated with training and culture, and breaking down our tribal stovepipes.

Ladies and gentlemen, thank you very much for your attention. I would now like to invite Chief of Air Force, Air Marshal Angus Houston, to close the conference.

# CLOSURE

## AIR MARSHAL ANGUS HOUSTON, AO, AFC

Distinguished guests, ladies and gentlemen, I will not go over what Air Vice-Marshal McLennan has just covered; I think he summed up the conference very well. Let me say, though, I am absolutely delighted with the outcome of this very important conference for the Air Force and, indeed, the Australian Defence Force. It has been a wonderful two days and I think we have had some really stimulating and insightful presentations from a variety of speakers and I would like to thank those speakers for the outstanding input to the success of this conference. So would you join with me in thanking the speakers for their contributions?

Group Captain Ric Casagrande, as many of you probably know, is the Director of the Air Power Development Centre and he and I sat down about ten months ago to work out what we might do with this conference. We decided that we would embark on this ambitious subject, 'Network Centric Warfare', and I said, 'Do you think it'll be a problem?' He responded, 'Oh no, no problems sir. We'll fix this one, it won't be a problem.' I saw him a couple of weeks later and I said, 'How is it going Ric?' He replied, 'Well, I'm actually off to the Middle East', and he disappeared to Baghdad and reappeared about two weeks ago. Like all good leaders in the Royal Australian Air Force, he gave the job to his staff to do and, of course, they have come up trumps. Sanu Kainikara, ably assisted by Sandra Di Guglielmo, has done an absolutely magnificent job in getting into the detail of this conference to ensure its great success. I am also very much aware that they led an outstanding little team, which included Roz Bourke who did a lot of the administrative support and Michelle Lovi who looked after all of the printing work. Group Captain Graham Bond—that ageless former Supply Officer who appears at all these events—and Wing Commander Maxine Dahl did a magnificent job in looking after our overseas guests and making sure that every detail was taken care of. Of course, No 28 Squadron, our Reserve Squadron here in Canberra, as always came to the party in strength and gave us great support. You probably all noted, with the situation we have in the world today, that we have a much enhanced security presence here provided by the Air Force Security Police personnel. I say to all of them, thank you very, very much for ensuring the success of this conference. The administration was simply magnificent and I would like all of you to join with me in thanking that wonderful team of people.

As I said at the very outset, these sorts of conferences do not happen without support from the industrial sector, our business supporters, and obviously prime amongst our supporters was Boeing Australia. Boeing was our principal sponsor. They have been very generous and they also provided a fantastic speaker and it has been great the support that we have had from them. Qantas has also supported us very generously and the other principal sponsor was, of course, Rolls-Royce who has been supporting events like this for the Air Force for many, many years. We also had Defence Force Credit Union, Defence Health and ID Warehouse. To all the sponsors, can I say again a very sincere thank you from me and the other members of the Royal Australian Air Force for your generous support in putting on this conference. So thank you very much to the sponsors.

To the moderators, Air Commodores Mark Lax, Stew Cameron, John Harvey and Chris Deeble, thank you very much for guiding the conference through the last two days. And to you, the audience, my thanks for your participation. You have been a good audience—I noticed what Lieutenant General Peter Leahy said about the way you can provide an objection to what is being said up the front; I have not seen too many people asleep—and to you well done.

Finally, to our distinguished overseas guests, it has been an absolute pleasure to have you here in Australia. I have really enjoyed meeting up with you all, talking to you and, indeed, furthering our relationships with all of your nations. It is always good to have that enriching quality of input from our overseas guests. To you I wish you all the very best on your return to your countries and a safe trip home. Thank you for coming.

The next time we do something like this will be at Avalon in March 2005, it will also include the Avalon Air Show. The whole Avalon Air Show has been moved to the right so it does not clash with other major events in Melbourne and I would invite all of our overseas guests to be strongly represented at what promises to be another great event on the Australian calendar.

At this point I think it is appropriate that I close the proceedings. It has been a magnificent two days and, again, my thanks to the Air Power Development Centre team for a fantastic job very, very well done. Thank you.

I now declare these proceedings well and truly closed.