Sea Power Series
2

Networking the Global Maritime Partnership

By Stephanie Hszieh, George Galdorisi, Terry McKearney and Darren Sutton

Sea Power Centre - Australia

NETWORKING THE GLOBAL MARITIME PARTNERSHIP

Cover image - courtesy of US Navy

National Library of Australia - Cataloguing-in-Publication entry:

Authors: Hszieh, Stephanie 1972 -
Galdorisi, George 1948 -
McKearney, Terry 1951 -
Sutton, Darren 1966 -
Title: Networking the Global Maritime Partnership
ISBN: 978-0-9925004-2-9
Series: Sea Power Series, No. 2
ISSN: 2202-8099

Subjects: Royal Australian Navy
United States Navy
Maritime Networking
Maritime Coalition Communications
Maritime Policy
Maritime Strategy
Maritime Security

NETWORKING THE GLOBAL MARITIME PARTNERSHIP

BY STEPHANIE HSZIEH, GEORGE GALDORISI,
TERRY MCKEARNEY AND DARREN SUTTON

The Sea Power Centre - Australia was established to undertake activities to promote the study, discussion and awareness of maritime issues and strategy within the Royal Australian Navy, the Department of Defence and civil communities at large. Its mission is:

- to promote understanding of sea power and its application to the security of Australia's national interests
- to manage the development of RAN doctrine and facilitate its incorporation into ADF joint doctrine
- to contribute to regional engagement
- contribute to the development of maritime strategic concepts and strategic and operational level doctrine, and facilitate informed force structure decisions
- to preserve, develop, and promote Australian naval history.

Comments on this volume or any enquiry related to the activities of the Centre should be directed to:

Director
Sea Power Centre - Australia
Department of Defence
PO Box 7942
Canberra BC ACT 2610
AUSTRALIA

Email: seapower.centre@defence.gov.au
Website: www.navy.gov.au/spc

Foreword

The challenges to our nations and navies on the world's oceans and seas have multiplied in our globalised world. Because of this, a global maritime partnership of navies netted together has a critical role to play in maintaining the rule of law on the world's oceans and ensuring the stability of the global commons upon which we all rely. Indeed, there are wide-ranging benefits in navies coming together to solve today's difficult and complex challenges of peace, crisis and war.

Drawing on their experience as naval operators and civilians embedded in the Australian and US military and naval laboratory systems, *Networking the Global Maritime Partnership's* authors examine the rich history of modern maritime coalition warfare as well as the equally rich history of maritime communications (and subsequent networking) between and among navies. They also expose the core reasons why navies have been especially challenged to network effectively in this still-new century.

The book's authors draw upon their experience working together to solve command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) challenges under the auspices of The Technical Cooperation Program (TTCP) - an inter-laboratory consortium among Australia, Canada, New Zealand, United Kingdom, and the United States (AUSCANNZUKUS) - to shed light on the challenges navies have in attempting to network effectively at sea. In addition to presenting the results of this six-year TTCP effort, they extrapolate the lessons learned from this work to inform a road ahead for enhanced networking among navies operating to secure the global commons.

Our experience of several decades of research, teaching, lecturing, presenting and moderating at a wide range of international academic, military, industry, naval and maritime venues has shown us that there is a vital need for navies to network successfully as they come together to form global maritime partnerships. This is not a passing fad or a *cause du jour*. Rather, it is a compelling imperative to make these partnerships even more robust and effective in ensuring the rule of law on the global commons.

Likewise, our work with senior government and naval and maritime officials in Australia, the United States, and other nations likely to unite in global maritime partnerships provides insight into the importance of tackling maritime threats cooperatively in naval coalitions. But we also have learned that while the 'will' is there, and while these nations and navies are aligned through doctrine, operating practice, tactics, techniques and procedures to work and network together at sea,

the technical means to realise the promise of 'network-centric warfare' - what Dr Norman Friedman has described as 'picture-based warfare' - throughout coalitions remains elusive. *Networking the Global Maritime Partnership* assesses the C4ISR challenges to achieving effective naval coalitions and outlines the ways and means to overcome them.

The book's authors build on an already-impressive body of work on global maritime partnerships and networking at sea in professional journals and publications in Australia, Canada, the United Kingdom, the United States and elsewhere, as well as conference proceedings in a wide-array of academic, industry, and military venues - an experience based on their wide-ranging military, scientific, and academic backgrounds. Importantly, *Networking the Global Maritime Partnership* does not offer a 'school solution' and instead provides an innovative and forward-leaning analysis of the course ahead for increased C4ISR connectivity between navies united as a force for good. They clearly break new ground in this vitally important area.

Dr Sam Bateman
Australia

Dr Scott C Truver
United States of America

PREFACE

Navies have always employed techniques to aid and improve communication and the exchange of information at sea but as technology advances, interoperability between partners – be they allies, coalitions or otherwise – becomes increasingly complex. This complexity results in a multitude of issues which continue to affect the success of networked operations. *Networking the Global Maritime Partnership* highlights the communication challenges associated with naval missions during coalition operations at sea. It also addresses the opportunities made available by effective communication networks.

The concept of a 'thousand-ship' navy proposed in 2005 by Admiral Michael Mullen, then US Navy Chief of Operations, recognised that in an era of fiscal austerity and shrinking naval fleets, nations will need to work together to protect the global maritime domain. Admiral Mullen's prescience is evident now as the major powers and other G20 nations grapple with reduced defence budgets.

Networking within coalitions is a critical enabler to achieving a global maritime security partnership. From an Australian perspective, effective naval networks between our traditional allies, the United States, United Kingdom, Canada, and New Zealand are vital to the success of future coalition operations. With our regional focus though, persistent or impromptu networks with our near neighbours are just as important.

Cooperation between navies, spanning the technical, procurement and operational spheres, is necessary to mitigate some of the current networking challenges as well as to seize the opportunities available from enhancing the effectiveness of information exchange. Readers interested in network centric warfare, and its future success, will benefit from this research and analysis. *Networking the Global Maritime Partnership* provides an excellent starting point for further discussion and research regarding this vital element of naval operations.

Captain Justin Jones, RAN
Director, Sea Power Centre – Australia
Canberra, May 2014

Acknowledgements

Special thanks must go to the *The Technical Cooperation Program* for enabling this research. The TTCP is a forum for defence scientists and engineers from Australia, Canada, New Zealand, the United Kingdom, and the United States to collaborate on science and technology issues.

Notes on Contributors

Stephanie Hszieh

Dr Stephanie Hszieh is a Corporate Strategy Group Strategic Analyst at the Space and Naval Warfare Systems Center Pacific, San Diego, California. She earned a PhD in political science from the University of Southern California.

George Galdorisi

Captain George Galdorisi, USN (Ret), is Director, Corporate Strategy Group, at the Space and Naval Warfare Systems Center Pacific in San Diego, California. He is a graduate of the US Naval Academy, and holds master's degrees from the Naval Postgraduate School (oceanography) and the University of San Diego (international relations). Additionally, he is a graduate of both the junior and senior courses at the Naval War College as well as the MIT Sloan School's Program for Senior Executives. He is the author of the *New York Times* Best-Seller, *Tom Clancy Presents: Act of Valor*. His forthcoming book (May 2014) *Out of the Ashes*, revives the Tom Clancy Op-Center series.

Terry McKearney

Mr Terry McKearney is the president and founder of The Ranger Group. He has spent the last twenty years analysing the organisational needs of contemporary military and public organisations. He has been particularly focused on the evaluation of command and control (C2) systems in joint operations. A retired naval officer whose service spanned the Vietnam era to the post–Cold War era, he holds master's degrees from the US Naval Postgraduate School and San Diego State University.

Darren Sutton

Dr Darren Sutton is Group Leader, Combat Systems Effectiveness and Analysis in the Defence Science and Technology Organisation. He is also the science and technology adviser to the Royal Australian Navy's Air Warfare Destroyer Project. Dr Sutton earned his doctor of philosophy in science (laser diagnostics for hypersonic flows) from the Australian National University.

Contents

Abbreviations

AAW	Anti-Air Warfare
ABCA	American, British, Canadian, Australian Armies
ABDA	American, British, Dutch, Australian
ABDACOM	American, British, Dutch, Australian Command
ABDAFLOAT	American, British, Dutch, Australian naval component
ACINT	Acoustic Intelligence
ADF	Australian Defence Force
AFCEA	Armed Forces Communications and Electronics Association
AG	Action Group
AIS	Automated Identification
AR	Arrival Rate
ARPANET	Advanced Research Projects Network
ASEAN	Association of Southeast Asian Nations
ASIC	Air and Space Interoperability Council
ASuW	Anti-Surface Warfare
ASW	Anti-Submarine Warfare
AUSCANNZUKUS	Australia, Canada, New Zealand, United Kingdom, United States
C2	Command and Control
C4I	Command, Control, Communications, Computers, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CANES	Consolidate Afloat Networks and Enterprise Services
CAP	Combat Air Patrol
CCEB	Combined Communications Electronics Board
CCRP	Command and Control Research Project

CDRE	Commodore
CEC	Cooperative Engagement Capability
CENTRIXS	Combined Enterprise Regional Information Exchange
CIE	Collaborative Information Environment
CIS	Communications and Information System
CMF	Combined Maritime Forces
CNO	Chief of Naval Operations
COP	Common Operational Picture
CRN	Contact Refinement Node
CS-21	*A Cooperative Strategy for the Twenty-first Century*
CSG	Carrier Strike Group
CTF	Combined Task Force
DARPA	Defense Advanced Research Projects Office
DEA	Data Exchange Agreements
DOD	Department of Defense
DSG	Defense Strategy Guidance
DSTL	Defence Systems Technical Laboratory
DSTO	Defence Science and Technology Organisation
EHF	Extremely High Frequency
ESG	Expeditionary Strike Group
EU	European Union
FIAC	Fast Inshore Attack Craft
FMS	Foreign Military Sales
FRAGO	Fragmentation Operations Order
GCCS	Global Command and Control System
GMP	Global Maritime Partnership
HA	Humanitarian Assistance
HCA	Humanitarian and Civic Action

HF	High Frequency
HQ	Headquarters
HVU	High Value Unit
ICT	Information Communications Technologies
IEA	Information Exchange Agreements
INTERFET	International Force East Timor
IP	Internet Protocol
ISR	Intelligence, Surveillance, and Reconnaissance
IT	Information Technology
J6	Deputy Chief of Staff for Command, Control, and Communications (Joint Staff)
JIE	Joint Information Environment
LACM	Land Attack Cruise Missile
LAN	Local Area Network
LCS	Littoral Combat Ship
MANA	Map Aware Non Uniform Automata
MAR	Maritime System Group
MDA	Maritime Domain Awareness
MEF	Marine Expeditionary Force
MIC	Multinational Interoperability Council
MIO	Maritime Interdiction Operations
MOCU	Multi-Robot Operator Control Unit
MOE	Measure of Effectiveness
MOP	Measure of Performance
MSG	Maritime Systems Group
MSSP	Malacca Strait Sea Patrol
NAMRAD	Non-Atomic Military Research and Development
NATO	North Atlantic Treaty Organization
NCMW	Network-Centric Maritime Warfare

NCW	Network Centric Warfare
NGEN	Next Generation Enterprise Network
NM	Nautical Mile
NNEC	NATO Network Enabled Capability
NTDS	Naval Tactical Data System
OEF	Operation Enduring Freedom
ONR	Office of Naval Research
OODA	Observe, Orient, Decide, Act
OOTW	Operations Other Than War
OPORD	Operations Order
OPTASK	Operational Taskers
PAAMS	Principal Anti-Air Missile System
PC	Personal Computer
PWO	Principal Warfare Officer
QDR	Quadrennial Defense Review
RAN	Royal Australian Navy
RBC	Reach back Cell
RF	Radio Frequency
RIMPAC	Rim of the Pacific exercise
RMA	Revolution in Military Affairs
ROK	Republic of Korea
RUSI	Royal United Services Institute
SHF	Super High Frequency
SIPRNET	Secure Internet Protocol Router Network
SM-6	Standard Missile (type) 6
SOA	Service Oriented Architecture
SPAWAR	Space and Naval Warfare Systems Command
SSA	Shared Situational Awareness

SSC	SPAWAR Systems Command
STANAG	Standardisation Agreement
TACSIT	Tactical Situation
TADIL	Tactical Data Link
TADIXS	Tactical Data Information Exchange System
TBS	Talk Between Ships
TDA	Tactical Decision Aid
TOI	Target of Interest
TOR	Terms of Reference
TP	Technical Panel
TTCP	The Technical Cooperation Program
US	United States
UAV	Unmanned/Uninhabited Aerial Vehicle
UCAV	Unmanned/Uninhabited Combat Aircraft
UHF	Ultra High Frequency
UK	United Kingdom
UN	United Nations
US	United States
USCENTCOM	US Central Command
USCYBERCOM	US Cyber Command
USN	United States Navy
USNI	US Naval Institute
USPACOM	US Pacific Command
UV	Unmanned/Uninhabited Vehicle
VHF	Very High Frequency
VOIP	Voice Over Internet Protocol

Introduction

The purpose of *Networking the Global Maritime Partnership* is to serve as a contribution to the ongoing dialogue regarding the global maritime partnership, and specifically, to address the challenges and opportunities associated with networking this partnership to enhance its effectiveness.

Real-world operations, especially in the Pacific Rim, have demonstrated that networking maritime forces is crucial to the effectiveness of operations that run the gamut from humanitarian operations, to insurgencies, nation-building, and state-on-state conflict. Additionally, these operations often involve nations and navies that come together at short – or no – notice and as a *necessary condition* for these operations to be successful, this networking must be immediately available and robust.

The central theme of this publication is that overcoming the technical challenges of networking maritime forces together is more daunting today than at any time in history. Why? Simply because unlike in the days when flag hoists or simple radio transmissions were all the networking that navies needed for effective cooperation, rapid technological change has reached nations and navies unevenly and has actually *impeded* the effective networking of coalition partners.

Before one can examine the technical challenges of networking maritime forces today, one must begin by understanding the history of coalition navies communicating and networking at sea in order to put the challenges - and the opportunities - surrounding networking coalitions at sea in the twenty-first century into the appropriate context. This history can then inform defence and naval policy experts, naval operators, acquisition professionals, scientists and engineers in all the nations and navies committed to maintaining the rule of law on the global commons through global and regional maritime partnerships.

Chapters One and Two explore the history of naval coalitions and communications in order to provide context for the technological revolution that is occurring within naval forces. Chapter One traces the history and importance of maritime coalitions for the past four hundred years. Coalitions have allowed allied naval forces to achieve military objectives when these objectives could not have been achieved by any one navy alone. In this post-Cold War era we suggest that maritime coalitions have become the *sine qua non* of successful naval operations.

As navies have been operating together for centuries, they have also been working to develop ways to communicate at sea. Chapter Two examines the evolution of naval communications from the age of sail to the development of network-centric warfare. This latter development, sometimes thought of as an artefact of the twenty-first century, seeks to harness the speed and connectivity offered by modern information communications technologies to make navies more effective in operations across the spectrum of conflict.

The global nature of today's naval operations has challenged navies to develop technologies to keep them connected and *networked*. For naval forces today, a necessary enabler of global and regional maritime operations is the suite of technologies supporting C4ISR (command, control, communications, computer, intelligence, surveillance, and reconnaissance) processes. The Royal Australian Navy (RAN), like many modern navies, has moved forward proactively in incorporating C4ISR technologies into its fleet. Chapter Three discusses and explores the importance of C4ISR technologies in allowing navies like the RAN to enhance their network-centric warfare capabilities.

As navies strive to adopt networking C4ISR technologies in their own fleets, real world maritime operations are revealing some of the technological challenges navies have in operating together. Chapter Four looks at modern day coalition operations and the issues that emerge when navies with disparate technological capabilities seek to operate together. Naval coalitions have often been plagued by political and operational challenges - for example the infighting between the Christian fleet commanders in the days before the Battle of Lepanto. However, a new challenge has emerged as individual naval forces work to enhance their information communication technologies to better network their own fleets. The technological mismatches that occur *between* navies can make information exchanges extremely difficult and may dissuade navies from operating together today and in the future.

While Chapter Four presents the technological challenges facing naval forces, Chapter Five proposes that one of the first steps for navies to work towards greater coalition interoperability must begin within the defence laboratories of these nations. The work of scientists and engineers at the defence laboratories of the AUSCANNZUKUS nations provide one example of what can be done to address the technical issues impacting coalition interoperability. The core of this penultimate chapter is TTCP where scientific and technical information is exchanged among member nations. The work of TTCP, as elaborated in the chapter, provides an example of how the 'wicked problem' of coalition interoperability can be addressed.

Chapter Six presents the concluding argument that the TTCP model provides the international naval community with a means to: 1) tap into the global marketplace of ideas where defence laboratories and academic institutions can collaborate to address technical issues; and 2) work towards a collaborative solution to provide network-centric coalition communications to all partner nations. To borrow the motto of the Combined Maritime Forces (CMF), network-centric coalition communications developed through collaborative exchanges will allow coalition partners to be 'Ready Together'.

1. Coalitions at Sea

The focus of this book is coalition communications in the maritime commons. Why is this important at a time when navies have been successfully communicating at sea for generations? To begin with, the need to communicate at sea has grown from one of simple communications between ships in a fleet to one of networked communications between each ship and shore commands, and the larger joint force. Secondly, the emerging international environment after the events of 11 September 2001 is evolving around the concept of global interconnectedness and the need for nations to work in 'cooperative action' to maintain the stability of the global economy.[1] *Australian Maritime Doctrine* notes that:

> Australia's strategic environment is most fundamentally shaped by the global distribution of power...the strategic environment is increasingly complex and interconnected, and the boundaries between international and domestic security issues are progressively more blurred.[2]

It is this increasingly interconnected environment that Australia and other nations are facing, one in which the maintenance of the global, regional and national economy has become a national security necessity. Coalition[3] operations at sea, while not a novel endeavour, have come into favour among nations at all spectrums of economic development - from the United States' Global Maritime Partnership Initiative to the Southeast Asian maritime partnership between Malaysia, Singapore, and Indonesia to patrol the Malacca Strait (better known as the Malacca Strait Sea Patrol (MSSP)).

Central to these international coalitions is the common need to meet military and political objectives where one nation could not accomplish them alone. This shared strength is an enduring feature of coalition operations as had been noted by Napoleon when he was said to have observed that, '[t]he only thing worse than fighting in a coalition is fighting against one'.[4] Paul T Mitchell noted that modern day coalitions have four characteristics: are often formed quickly; are commonly formed to secure international stability and support the maintenance of peace; are not hierarchical or have limited hierarchical structures; and are not guided by 'strong national interests'.[5]

A Brief History of Coalitions

Some think of coalition warfare as something new, an artefact of the twentieth century, when nations banded together to fight aggression and totalitarianism. But this is not the case. Coalition warfare goes back over two millennia. The Peloponnesian War pitted a coalition built around Sparta against one built around

Athens in a duel for mastery of what was essentially the Western world at that time. Importantly, as Thucydides relates in *The History of the Peloponnesian War*, and as Victor Davis Hanson describes in *A War Like No Other*, much of this coalition warfare occurred at sea.[6] Coalition warfare at sea has prevailed through countless conflicts to the present day.

Naval Coalitions of the Age of Sail and Beyond

The 'Age of Sail,' a period beginning in roughly the seventeenth century, can be thought to mark the beginning of modern naval coalitions for several reasons. During this period, the nation state matured into its modern form, with the establishment of permanent navies. This paralleled the development of world-wide trade routes through the colonisation of the New World and new alliances formed in the corresponding shift in global power. Naturally, these alliances had a naval component; navies would not only fight against each other, but alongside each other. Naval coalitions evident during the age of sail and steam engines continue to be used as nation-states organise around alliances to promote their common political and military aims.

Coalitions of the Nineteenth Century

Naval coalitions of the nineteenth century were typified by the balancing of powers between the great empires of that era and the protection of colonial assets. The Boxer Uprising of 1900 saw the great powers of Europe, the United States, and Japan join together to halt Chinese attacks on foreigners and foreign properties. The Boxers were a nationalist movement in China that organised to remove the foreign presence in the predominantly coastal areas of China. Western military forces were eventually called in as the Boxers extended their violence to killing foreigners. One notable incident was in May 1900 when several Belgian and French railway engineers were killed fending off armed Chinese in the city of Tianjin. In response to the outbreak of attacks '337 British, French, Italian, Japanese, Russian, and United States marines and bluejackets were sent to Beijing to protect their citizens and properties in that area'.[7] Additionally, Western and Japanese naval vessels in the waters of northern China joined together in a loose coalition to guard against Boxer attacks and piracy.[8]

The height of the naval activity to protect Western assets in China during the Boxer Uprising was the capture of the forts at Dagu, the Chinese stronghold that limited the foreign powers from supporting their establishments in Tianjin and Beijing. The multinational naval coalition of British, Russian, French, German, Japanese, Austrian, and US battleships and cruisers laid siege on the Chinese fortifications

on the coast of Dagu.[9] The capture of the Dagu forts served as the foundation for the foreign military campaigns that followed and eventually brought to an end the Boxer rebellion. It also laid the groundwork for future coalitions that proved to be important during the next great power conflict - World War I.

Anglo-Japanese Alliance (1914-18)

The political/military environment leading up to World War I saw the British Navy massing its forces in home waters to meet the growing threat of German naval power, leaving a small naval force in the Pacific and the Mediterranean.[10] This move forced Britain to look to its allies to provide the forces needed to support its fleet in these areas and Japan was the ally of choice to provide support to the Royal Navy in the Pacific. The British were wary of entering into an alliance with the Japanese as it slowly expanded its sphere of influence in China and the Pacific region. However, the growing threat of German expansion of its naval operations in the Pacific convinced the British that they needed Japan as an ally in the war effort.[11]

The Anglo-Japanese coalition began with the Siege of Qingdao (Tsingtao), China where Britain and Japan entered into joint operations to attack the base of the German Far Eastern squadron.[12] This was also the first time in military history that an aircraft carrier was successfully attacked by opposing aircraft.[13] In addition to blockading operations, the Anglo-Japanese naval cooperation also included tracking down elements of the German navy operating in the region.[14] Coalition operations also extended to not only operating together but also sharing of resources and personnel. During that time, the Japanese 'were given use of British naval bases in the Far East, notably Singapore' and Japanese crews manned two British destroyers to support the anti-submarine efforts against the Germans.[15] The Japanese also opened up their shipyards to the French 'to build a class of 12 destroyers based on a Japanese design'.[16]

World War II: The Pacific (1941-45)

The Pacific theatre in the opening years of World War II provides another example of navies banding together to improve their odds in battle. World War II was a war of coalitions - primarily the allied forces of the United States, the United Kingdom and the Commonwealth states, and eventually the Soviet Union against the Axis forces of Germany, Italy, and Japan.

The story of the American, British, Dutch and Australian joint force is that of a coalition formed to counter Japan as it conducted its stunning sweep down Asia while the core of the Allied forces were focused on the European front. Known as the ABDACOM, the joint command was established in 1942 to provide a defence

of allied territories in the Pacific region.[17] The ABDACOM naval component (ABDAFLOAT)[18] comprised of the US Asiatic Fleet along with ships from British and Dutch navies.

The objective of ABDACOM was to protect the Dutch East Indies and Australia from the Japanese. However, the coalition was faced with competing national interests and limited resources as air support was sparse and the sheer size of the Pacific Ocean greatly stretched allied capabilities. Admiral Thomas C Hart, commander of the naval element of ABDACOM had to deal with the conflicting priorities of coalition partners:

> In the prewar conferences…it became clear that the Royal Navy was worrying less about defending Java than about saving its imperial crown jewel, Singapore…Long before war began, the Americans and the British had debated the merits of holding Singapore. The Americans considered it hopeless once Japanese land-based airpower came to bear on it.[19]

The Cold War

Although the Cold War conflict was predominantly a political and military contest between the superpowers, the United States and the Soviet Union, it was very much a test of wills between two international coalitions. Bradford Lee, professor of strategy at the US Naval War College, notes that the 'Cold War was a peculiar type of coalition struggle involving naval powers'.[20]

Lee adds that the staying power of the Western-US led alliance was built on the alliance's naval superiority.[21] The earliest naval conflict of the Cold War era provides an example of Lee's argument that the better formed maritime coalition of the US and allies were able to maintain sea control in one of the 'hot' conflicts of the time. The Korean conflict is known for the brutal land battles in the freezing mountain passes of the Korean peninsula. However, the ability of US and coalition navies to control the waters around Korea made it possible for the troops on the ground to win back ground south of the 48th parallel. The initial invasion of the Korean peninsula by communist troops had overwhelmed the poorly distributed forces of the Republic of Korea (ROK) and Seoul soon fell to the Communists.[22] The small ROK Navy was also unable to stop enemy ships from resupplying troops on shore.

The arrival of the US Seventh Fleet and naval vessels from the United Kingdom, Australia, New Zealand, Canada, Cambodia, France, the Netherlands, and Thailand, helped to ensure that the Communist forces could not be reinforced by sea.[23] Coalition naval partners also provided additional personnel to assist in the land war as seen by the example of teams of New Zealand sailors and Royal Marines who conducted raids along the North Korean coast.[24] The presence

of the Seventh Fleet also kept China and the Soviet Union from expanding the conflict to Taiwan.[25] In addition to providing air support and shore bombardment the coalition naval force:

> ...denied the enemy use of the sea to transport troops and supplies. Control of the sea also allowed the U.N. command to threaten amphibious landings in the rear of the communist armies fighting along the 38th parallel.[26]

While the Korean conflict showed the power of the emerging Western alliance, it also served to prompt the Truman administration to support the development of the North Atlantic Treaty Organization (NATO).[27] During the Cold War period much of the focus of NATO and the Western alliance was on checking Soviet encroachment across Europe and building a credible nuclear and conventional deterrent. A key to NATO's strength against the Warsaw Pact was, as Lee argues, the naval superiority of the West:

> The Cold War strategy of containment, in particular, also depended heavily on naval superiority to project power across vast seas.... command of the seas provided the United States with a high level of security against conventional attack and safeguarded a new international economic order that made association with the US all the more attractive to its allies in Europe and Asia.[28]

The Post-Cold War Era

With the thawing of the Cold War, coalition operations at sea regained importance as former adversaries began working together. One notable sign of the changing geopolitical environment after the fall of the Soviet Union in 1991 was the joint naval exercises off the Norwegian coast that comprised NATO vessels and those of the former Warsaw Pact - Russia, Lithuania, and Poland.[29]

Operation DESERT STORM presented the first major post-Cold War test of the ability of military forces in general - and naval forces in particular - to operate in concert with large numbers of coalition partners. As the world's militaries and navies assimilated the lessons of DESERT STORM, there was increasing recognition that the command, control, and reconnaissance systems that undergirded the entire coalition war effort were not only the most important key to victory, but also needed to become more adaptable to link partner militaries and navies.[30] Concurrently, the world's major maritime powers also began to realise that the world was rapidly becoming a place where 'brush-fire wars', would require agile coalitions of nations operating in virtual 'pick-up games' to deal with emergent crises.[31]

Why Coalitions Today?

As the saying goes, the more things change, the more they stay the same. Coalitions remain an important part of political and military activities. However, the need for coalition operations in today's world has evolved. While today's naval coalition operations are similar to those of the past - ships and crews of different nation-states working together in a common mission - the political impetus behind coalitions today has taken on a global perspective.

The US Navy recognised that when Admiral Michael Mullen, then US Navy Chief of Naval Operations (CNO), proposed the 'thousand-ship navy' concept at the Seventeenth International Seapower Symposium in 2005. The thousand-ship concept still resonates in the US Navy as noted by Admiral Jonathan Greenert, US Navy CNO, in a speech at a 2012 event hosted by the Association of the United States Navy when he said, 'We're not at 1,000 around the world, but...the 1,000-ship navy, I think, is alive and well'.[32]

The thousand-ship navy concept has been incorporated into the Global Maritime Partnership Initiative outlined in the US Maritime Strategy - titled *A Cooperative Strategy for 21st Century Seapower* (CS-21). CS-21 notes that preventing wars is as important as winning wars and the key to prevention is strengthening and building alliances and partnerships.[33] This is not to say that the US Navy is moving away from its core warfighting duties, as noted in the CNO's Sailing Directions, the number one job of the Navy as the first tenet is still 'Warfighting First'. The second tenet, 'Operate Forward', touches on the importance of maintaining and building partnerships and alliances to 'improve our ability to cooperate with regional partners in maritime security operations'.

The growing importance of maritime cooperation and the more general coalition operations is also emphasised in the US Defense Department's Defense Strategic Guidance (DSG) - also known by the title *Sustaining US Global Leadership: Priorities for 21st Century Defense*.

> Building partnership capacity elsewhere in the world also remains important for sharing the costs and responsibilities of global leadership. Across the globe we will seek to be the security partner of choice, pursuing new partnerships with a growing number of nations...whose interests and viewpoints are merging into a common vision of freedom, stability, and prosperity.[34]

As Geoffrey Till notes, '[g]lobalisation is not entirely new, nor has it always been secure',[35] and the global nature of this current international system has made cooperation at the global level an important part of international security schemes.[36]

US Defence Priorities and National Security

In the US, the Department of Defense is examining areas to cut to provide for a sustainable force structure with a federal budget that is facing increasing social obligations and debt. In May of 2010, then Secretary of Defense Robert Gates ordered all the civilian and military departments to take a hard look at their operations and reduce overhead. In the Secretary's words:

> to convert sufficient 'tail' to 'tooth' to provide the equivalent of the roughly two to three percent real growth - resources needed to sustain our combat power at a time of war and make investments to prepare for an uncertain future.[37]

The efforts to posture the US military to meet future reductions of the defence budget and scope future missions continued under then Secretary of Defense, Leon Panetta. In an extraordinary move to ensure that the future US military force will be able to meet future challenges, the White House, Department of Defense, and the Services collaborated on an overarching blueprint to 'help guide decisions regarding the size and shape of the force over subsequent program and budget cycles'. The overarching blueprint is found in the DSG. Released in early 2012, the DSG serves as the overarching strategic document for planning the future force. The key elements of this keystone document are:

- Sustaining global presence; renewed emphasis on Asia together with continued focus on the Middle East; maintaining our commitments and evolving our presence in Europe and building innovative, low-cost, small-footprint approaches to partnership around the world.
- Protecting new capabilities and investments to respond to the changing nature of warfare; preserve lessons, capabilities and expertise of the past ten years; and ensuring our technological edge to meet future challenges.
- Aligning size and composition of forces to be capable of a range of missions and activities.
- Ensuring reversibility to maintain the ability to surge, regenerate and mobilise to counter any threat, while preserving our industrial base so we are able to address unforeseen challenges.

A key part of the strategy for twenty-first century defence is the maintenance and development of international partnerships. In an address delivered at the US Institute of Peace in 2012, then Secretary of Defense Leon Panetta articulated the US strategic focus on what the *DSG* described as 'building innovative, low-cost, small-footprint approaches to partnership around the world'.

> In order to advance security and prosperity in the 21st century, we must maintain and even enhance our military strength. But I also believe that the United States must place even greater strategic emphasis on building the security capabilities of others. We must be bold enough to adopt a more collaborative approach to security both within the United States government and among allies, partners, and multilateral organizations.[38]

One area that is seeing significant growth in strategic military partnerships is the Asia-Pacific region as the US begins its rebalance. The DSG formalised the US rebalance to the Pacific and while this move is part of a larger 'whole of government' strategy of engagement, the US military has a significant role in the effort. As US forces draw down from Southwest Asia, a number of the combat forces will be or are currently being reassigned to the Pacific. The most notable move is the stationing of 2,500 US troops in Australia - the first being over one hundred US Marines stationed in Australia's northern coastal city of Darwin in April 2012 to begin a six month rotation and engagement with the Australian Defence Force (ADF).[39]

Admiral Samuel J Locklear III, commander US Pacific Command (USPACOM), spoke with the Armed Forces Communications and Electronics Association (AFCEA) in late 2012 and provided an overview of the preparations underway in USPACOM's area of responsibility. In the interview, Admiral Locklear called out other notable reassignments to the Asia-Pacific region for the joint force: the return of the III Marine Expeditionary Force (MEF) to Japan; the alignment of I MEF to the region; and the realignment of the US Army's I Corps as they were previously assigned to Southwest Asia.[40]

The US reorganisation of military forces in the Asia-Pacific region is also focused on the development of strategic partnerships as is highlighted in the *DSG.*

> Our relationships with Asian allies and key partners are critical to the future stability and growth of the region. We will emphasize our existing alliances, which provide a vital foundation for Asia-Pacific security. We will also expand our networks of cooperation with emerging partners throughout the Asia-Pacific to ensure collective capability and capacity for securing common interests.[41]

At USPACOM, the need for strengthening historical alliances and building new partnerships has made coalition communication a priority for their J6. In an interview with *SIGNAL* magazine, Brigadier General Mark Hicks, USAF, director of J6, USPACOM, noted that roughly one-third of his effort is focused on multinational communications, interoperability and cyber security.[42] The USPACOM J6 focus on coalition communication is highlighted in two efforts - the development of the Joint Information Environment (JIE) Increment Two and USPACOM's future information

technology infrastructure. According to *SIGNAL* magazine, the second increment of the JIE will feature a 'solution for coalition communications'.[43]

> Through JIE, the plan is to create affordable, scalable information-sharing networks quickly for whatever coalition needs them at a certain time. Then when missions end, the networks are disestablished and reconfigured for a different set of partners just as quickly.[44]

Brigadier General Hicks is also looking at lessons learned from USCENTCOM's coalition networks to inform the building of USPACOM's future information technology architecture.

Coalition communications is also an important part of the Navy's support of the US focus in the Asia-Pacific region. In addition to increasing the number of ships and aircraft in the region, the US Navy will be also expanding operations with regional partners. CNO, Admiral Jonathan Greenert, noted in a November 2012 article in *Foreign Policy* that the US Navy will 'expand cooperative air surveillance operations with regional partners' as it also increases its training and exercises with coalition partners.[45]

Admiral Greenert noted that:

> The Asia-Pacific will become increasingly important to our national prosperity and security. It is home to the world's largest and most dynamic economies, growing reserves of natural resources, and emerging security concerns. Naval forces, with their mobility and relevance in peacetime and conflict, are uniquely poised to address these challenges and opportunities and sustain our leadership in the region. With our focus on partnerships and innovative approaches, including new ships, forward homeporting, and rotational crewing, the Navy can rebalance toward the Asia-Pacific while being judicious with the nation's resources. We will grow our fleet in the Asia-Pacific, rebalance our basing, improve our capabilities, and focus intellectually on the region. This will sustain our credibility to deter aggression, preserve freedom of maritime access, and protect the economic livelihood of America and our friends.[46]

This is consistent with what Australia and the ADF have long recognised. In 2006, Vice Admiral Russ Shalders, the Australian Chief of Navy, announced the adoption of the GMP concept as one that would best represent the way the RAN will likely operate in the future.[47] In his 2007 *RUSI* article, Vice Admiral Shalders noted that:

> From the perspective of the RAN, we look favourably on any initiative that increases maritime security awareness and co-operation – this is the true value of the '1000-ship Navy' concept.[48]

The importance of naval coalitions to Australia's defence is noted in the 2009 Australian Defence White Paper, *Defending Australia in the Asia Pacific Century: Force 2030*. The publication notes that:

> Australia's defence policy…entails the maintenance of alliances and international defence relationships that enhance our own security and allows us to work with others when we need to pool our resources…this defence policy means that we must have the capacity to lead military coalitions where we have shared strategic interests at stake with others…and make tailored contributions to military coalitions where we share wider strategic interests with others.[49]

The ADF has readily understood the importance of balancing the need for national security and engaging in the larger international system. Senator John Faulkner, the then Minister for Defence, reiterated the ADF's posture in his speech at the Pacific 2010 Maritime Congress and International Maritime Exposition in Sydney:

> …while the principal task for the ADF is to deter and defeat armed attacks on Australia, the ADF must also be ready and able to contribute to stability and security in the South Pacific, to military contingencies in the Asia-Pacific region and more broadly, in support of efforts by the international community to uphold global security and a rules-based international order, and to respond to humanitarian crises at home and abroad.[50]

Australia's 2013 Defence White Paper further reinforces the importance of naval coalitions by highlighting that Australia and the United States agreed:

> to explore opportunities in the long-term for enhanced cooperation… reflected in… investments in technology and weapons systems, and operational plans and tactics.[51]

Other members of the international community have also noted the need for greater cooperation at the international level given the growing interdependence of nations on the global economic system. The Royal Navy's First Sea Lord, Admiral Sir Jonathon Band, has argued that the Royal Navy should accept sacrificing quality for quantity if it is to maintain a surface fleet of sufficient size to contribute to maritime security operations on a global scale.[52]

Singapore, a regional partner, notes in its national defence document - *Defending Singapore in the 21st Century*:

> A stable international environment is necessary for Singapore's future security and progress, and we will have to play our part to build a peaceful regional and global order in the new century. The SAF [Singapore Armed Forces] will do more in the area of defence diplomacy. It will develop the capability to inter-operate with friendly forces and work with other armed forces to strengthen multilateral defence co-operation.[53]

Singapore's Defence Minister, Dr Ng Eng Hen, highlighted the importance of international cooperation in his speech at the 11th IISS Asia Security Summit (aka Shangri-La Dialogue) in June of 2012:

> Our common security challenges are often transnational and as we have witnessed can overwhelm resources occasionally. No single country has the resources or ability to provide lasting solutions. We will have to pool resources and synergise efforts...This generation is witnessing significant change in the global order and the new security challenges that come with it. We will need more effective institutions and mechanisms that provide both clear rules and leadership for the common good. In this vein, we must commit to working together to building stronger international institutions and constructive partnerships at both the bilateral and multilateral levels, based on shared interests, aspirations and principles.[54]

The Japanese Ministry of Defense's *Defense of Japan 2012*, notes that:

> Dependence on foreign trade for resources and food is particularly high, and maintaining peace and cooperation in the international community is of tremendous importance to Japan, as it places the foundation for its development and prosperity on free trade. For this reason, Japan is working to strengthen bilateral cooperative relationships such as the Japan–U.S. alliance while actively advancing regional cooperation in the Asia-Pacific region and with the United Nations, and to prevent and resolve conflicts and disputes, develop economically, promote arms control and disarmament, ensure maritime security, and enhance mutual understanding and trust.[55]

Globalisation, financial constraints, sustainable force structures, international commitments, and personnel/skill shortages are leading nations to consider coalition efforts as viable solutions to meet national and international security challenges. As Till notes in his assessment of the state of the Royal Navy, '[r]esponding to financially induced shortages mandates working in coalitions of the willing'.[56] The 2009 Australian Defence White Paper notes that:

> Coalitions are becoming increasingly important means of dealing with many security challenges…Such coalitions are vehicles by which different countries can pool their resources according to their comparative military strengths and capacity to contribute.[57]

The RAN provides the ADF with that capability to build cooperative security to maintain what Senator Faulkner described as 'rules based international order'.[58] The RAN capability to take the lead in coalition operations is seen in numerous humanitarian missions and coalition-oriented exercises such as RIMPAC.[59]

This tradition of cooperation and coordination has enabled navies to operate together nearly seamlessly for more than a century, including two world-wide conflagrations where they demonstrated the ability to achieve complete mastery of the sea that enabled the defeat of the enemy and hastened the end of both wars. Today, globalisation and the presence of a new generation of threats on the high seas, the littorals, and the near-shore land areas, demands even closer cooperation among navies with which they seek to partner.

Naval coalitions today tend to be heterogeneous in the types of navies represented and concentrate the focus on 'diplomatically isolated adversaries, so that strategic success requires at least two offensive prongs: one military and the other diplomatic'.[60] The types of operations of naval coalitions have also expanded to include disaster relief and humanitarian missions. For instance, the US Navy's Pacific Fleet developed the Pacific Partnership in 2005 to 'execute a variety of humanitarian and civic assistance (HCA) activities throughout the Pacific Fleet area of responsibility'.[61]

Pacific Partnership includes not only US Navy ships but also ships and personnel from the Japanese Maritime Self Defense Force, the Royal Australian Navy, the Indonesian Navy, US State Department entities, and non-governmental organisations. As noted by then-Commander of the US Pacific Fleet, Admiral Patrick Walsh:

> The world we live in today is more interconnected than before and history provides a window into the future, as it has demonstrated the importance of cooperation and collaboration when facing common challenges such as natural disasters. By working together, we are better prepared to overcome adversity and help each other in times of need.[62]

The Combined Maritime Forces (CMF) in operation in the maritime areas from the Arabian Gulf to the Suez Canal provide another example of the changing nature of naval coalitions to meet the challenges of a globalised international system. The CMF 'conducts Maritime Security Operations (MSO) in accordance with international law and relevant United Nations Security Council Resolutions [to]

counter violent extremism and terrorist networks'.[63] Within the CMF there are three Combined Task Forces - CTF 150, 151, and 152 - operating from the Red Sea to the Horn of Africa and involving naval forces from 24 nations.

What is noteworthy of the CMF is the contribution and leadership of smaller navies in these efforts.[64] For example:

- CTF 150, operating in the Red Sea, Gulf of Aden, Indian Ocean, Arabian Sea, and the Gulf of Oman. CTF 150 has been commanded by Australia, France, Netherlands, the United Kingdom, Canada, Germany, the United States, Spain, and Pakistan.
- CTF 151 operates in the Gulf of Aden and Somali Basin to deter, disrupt and suppress piracy and involves naval forces from NATO, EU, and other nations. CTF 151 has previously been commanded by Singapore, Turkey, the United States, and the Republic of Korea.
- CTF 152, in the Arabian Gulf, works with the Gulf Cooperation Council (GCC) partners in order to prevent destabilising activities. CTF 152 has previously been commanded by Australia, Bahrain, Italy, the United Kingdom, the United States, and Kuwait.

The successful RAN deployment as part of the joint force in the 1999-2000 International Force East Timor (INTERFET) reflects the growing importance of coalition operations to the RAN and of its coalition building capabilities to the ADF. INTERFET was a United Nations (UN) sanctioned international effort to provide stability and humanitarian aid to the beleaguered East Timor that was facing political and humanitarian crisis as it struggled to gain independence from Indonesia.[65] On request from the UN, Australia took the lead in organising this international force to 'provide a peaceful and secure environment in which the UN could conduct humanitarian assistance and nation building'.[66] The international force grew eventually to comprise 22 nations, including the United States, Canada, France, Italy, New Zealand, and Malaysia.

Part of the success of INTERFET was the strong coalition and command system that was built by the naval forces involved. In an interview with the US Naval Institute's magazine, *Proceedings*, the then–Chief of the Australian Navy, Vice Admiral David Shackleton, noted the unique ability of RAN and all navies to cooperate:

> …navies can meet almost anywhere. You can talk on a radio and you can set up an arrangement. Navies…are very good at forming and doing business in a Coalition way that I think armies and air forces find difficult.[67]

However, coalition operations for RAN and other navies are challenging as issues such as information sharing require great attention and trust. The INTERFET

experience showed that there is still much more work that needs to be done at the technical and policy levels to smooth out coalition interoperability. For instance:

> …even for the RAN and U.S. Navy, despite years of working together and operating compatible equipment, high-level interoperability did not just happen. One might have expected cryptographic commonality to be a C4I staple, but even maintaining this aspect was still found to require an inordinate amount of time and effort.[68]

The Challenge of Coalitions

The RAN's experiences with INTERFET in early 2000 shows how far naval coalitions have come from the age of sail and how much more work needs to be done to meet the growing needs of the international community. One area of special focus we will highlight in succeeding chapters is the importance of coalition communications and networking interoperability at the multinational coalition level.

Australian Maritime Doctrine defines interoperability as 'the ability to operate in synergy in the execution of assigned tasks'.[69] The need for members of a multinational coalition to communicate and exchange information is an enduring issue, but has taken on greater importance in this age of computers. During the period of World War I, one method of communications interoperability at the coalition level was through the exchange of sailors to learn another navy's signalling systems, which occurred when the United States adopted the British signalling methods.[70] In World War II, similar personnel exchanges occurred between US and British navies to synergise communications and information exchanges between coalition partners.[71]

During DESERT STORM, communications interoperability emerged as a key coalition issue as myriad communications systems had to be maintained and monitored. One problem was that smaller navies with limited satellite systems had difficulty keeping up with the large amount of data managed by the systems employed by larger navies such as the US Navy, and that many of these systems were not even interoperable with each other. For example:

> Misalignment between the operating standards for Link 11 between the US Pacific Fleet, with which the Australians operated, and the Europeans, who worked to the relevant NATO STANAG [Standardization Agreement], meant that the Australian destroyer *Brisbane* found she could not operate in the Link without corrupting the system of the British *Gloucester*. A solution in the form of a software patch to *Brisbane*'s combat data system was rapidly developed - within only 18 hours - by Australian shore authorities.[72]

With the advent of combat data systems and sophisticated naval weaponry, communications interoperability has become an important - if not central - part of effective coalition operations.[73] As Rear Admiral James Goldrick, RAN noted in his assessment of multinational naval operations in the 1990-91 Gulf War:

> [a]s early as 1961, naval tactical data links - the key ones later designated Link 11 and Link 14 - were the subject of a NATO Standardization Agreement (STANAG) and combined development work continued as more and more navies adopted combat data systems.[74]

The leaders of major navies recognise the importance of coalition interoperability. The former Australian Chief of Navy, Vice Admiral Shalders, once noted that Australia has adopted a doctrine of naval cooperation that will lead to 'a maritime neighbourhood watch scheme' involving joint exercises with Russia and China.[75] This interest spreads beyond traditional naval allies to include emerging regional and global naval powers such as India who are exploring the potential benefits of sharing information about maritime threats and situations.[76]

The importance of the ability to communicate with coalition partners transcends warfare and impacts coalition naval partners in literally every endeavour. This was dramatically demonstrated in December 2004 and early 2005 during the tsunami relief efforts in the western Pacific region where 18 nations worked together, primarily on and from the sea, to deliver relief supplies from naval vessels.[77] Interviews with naval officers involved in that effort indicated that while the forces ultimately got the job done, coalition communications at sea remains an ongoing challenge.

But policy decisions to effectively network coalition navies must be supported by the technological means to do so. And in an era when the majority of coalition naval operations may well be 'pick-up games', this technology must be devised to enable various combinations and permutations of naval coalitions to operate together effectively. This is an area fraught with many challenges - challenges well-known to the technical, policy and military communities but not yet solved.

2. A Brief History of Naval Communications

From the Flag to the Net

The focus of this chapter is on coalition communications; how far naval forces have come in communicating at sea, and some of the challenges that navies still face. The term communications, as it relates to maritime affairs, has two meanings. The first meaning refers to the sea lanes encircling the globe. Communications in this regard refers to the means of movement of commercial goods and services along with military supplies and troops across the world's sea lanes. The second meaning of communications at sea refers to what *Webster's Dictionary* defines as 'a process by which information is exchanged between individuals through a common system of symbols, signs, or behaviour'.[78] This meaning of communications with a small 'c' is what this chapter will address - the continuing evolution of how maritime forces exchange information at sea.

The key part of our definition of communications is 'information exchange' - the ability to exchange information between members of one nation's naval force or across a maritime coalition.[79] In the arena of naval warfare, communications is needed to maintain dominant battlespace awareness - to know where your enemies are and where your own forces are arrayed. Out of this knowledge comes the ability to plan to defeat the enemy. The Duke of Wellington aptly noted:

> All the business of war, and indeed all the business of life, is to endeavour to find out what you don't know by what you do; that's what I call guessing what's on the other side of the hill.[80]

Since the beginning of time, commanders have tried to guess 'what is on the other side of the hill' and as part of the effort, have developed means of communication to build a common tactical picture of the battlefield.

The earliest communications at sea were rudimentary, consisting of shouts of command from ship-to-ship to the lighting of signal fires on board to signal the start of action.[81] Naval communications in the age of galley warfare were rudimentary as tactics were basic.[82] Galleys were usually lined up in an optimal formation to ram the opponent's ships and it was up to the individual galley to hit the target and survive the melee that followed. This was the nature of naval warfare from the time of the Greco-Persian war 480-479 BCE to the last great galley war in 1571 when the Christian fleet of galleys clashed with the galleys of the Ottoman Empire at the Gulf of Lepanto. By that time, shipbuilding in the Christian nations had evolved to include galleasses or galleys that carried cannons. At Lepanto, the Christian fleet had six of these galleasses and a total of sixty cannons that surprised and

destroyed the Turkish fleet.[83] The age of the galley had ended and the need for a ship that could handle the new cannon warfare at sea brought about the age of the sailing ship.[84]

Sailing ships made it possible to expand the area of operations from coastal waters to the open sea and thus led to the development of more complex means of naval communications. With ships operating at greater distances from each other and from the homeport, commanders found greater need to develop communications systems to help them maintain awareness of the battlespace and of their fleet. The invention of the telescope and the binoculars in the early 1600s also enabled ships to communicate with each other at greater distances.[85] The primary means of communication in the age of sailing ships were signal flags that were used to convey simple instructions and warnings to the fleet.[86]

In addition to signal flags, cannon fire, lanterns, and messages sent by small boats between ships were also used to communicate commands or information.[87] Commands were conveyed by a series of flags or a single flag in accordance to a common signal book. For instance, in the 1730s the commander-in-chief of the British fleet in the West Indies, Admiral Edward Vernon, used a 'red flag at the main topmast head' to signal the fleet to form the battle line.[88] More detailed information from the admiral of the fleet to the rest of the fleet officers was conveyed by a messenger on a small boat.

Admiral Nelson took advantage of the flag signalling techniques to obtain a tactical picture of the French and Spanish fleet harboured at Cádiz. In the lead up to the Battle of Trafalgar (1805), Nelson had positioned his fleet out of sight of Cádiz in order to trick the combined fleet of French and Spanish ships to leave port.[89] From around 43nm (UK) away, Nelson was unable to keep the enemy fleet in sight. To compensate for this he established an information relay system of frigates that would pass back information on the movements of the enemy fleet.[90] The method of communications was a combination of flag signals based on Rear Admiral Popham's numerical flag system and night signalling - usually a series of lanterns set at agreed patterns.[91] The relay system allowed Nelson to obtain a better picture of the French and Spanish fleet disposition than it had of the British fleet. The combined fleet under the command of Vice Admiral Villeneuve was not able to maintain similar awareness of the British as they lacked deployed scout ships because of the earlier British blockade; they could only see to the horizon from their positions in Cádiz harbour.

Nelson's ingenuity in developing his information relay system provided him a view of the pending battlespace that allowed him to position his fleet to intercept Villeneuve before he could escape. However, the relay system was cumbersome as it took two hours for the signal that the enemy ships were leaving port to be relayed from one British ship to another to reach Nelson.[92] The time delay and the

inability to have a speedy two-way conversation produced a less than accurate picture of what Villeneuve's fleet was doing as they were leaving Cádiz.[93]

'The enemy's ships are coming out of port' was all the information Nelson received and since a reply back to ask about more details would have taken hours, Nelson had to assume that Villeneuve's fleet was heading for the Strait of Gibraltar and immediately set course to intercept.[94] That Nelson acted correctly on such limited information highlights the soundness of his pre-action planning. Had the successful execution of his plan required more information or had he needed to issue further guidance to either his observers at the port or his battle line, his communications structure might well have failed him.

Naval Communications in the Electronic Age

The Industrial Revolution ended the domination of the sailing ship in naval forces as it introduced the steam engine, the iron hull, and eventually electronic communications to naval warfare.[95] These advancements in naval technology allowed ships to conduct more complex manoeuvres and allowed them to travel faster than when they were at the mercy of the wind.[96] The adoption of electricity in naval warfare helped to quicken communications as naval communications between ship and shore and between ships before the electric telegraph typically took weeks or months.

> … the United States Navy's Pacific Squadron had to communicate with the Navy Department in Washington by dispatch vessel sailing round Cape Horn…Consequently in 1846 they did not know of an outbreak of war with Mexico until an officer travelling overland managed to get a message through privately.[97]

The introduction of the telegraph promised instantaneous communications across vast distances. No longer would messages take months to traverse continents as telegraph cables and networks made it possible for messages to be relayed in days. The Victorians eagerly embraced the telegraph as something that was 'faster and better' than waiting for newspapers to arrive via ship and something that would provide them the 'news of the home islands' instantly and without the multi-week time delay. However, this new technology had a downside: telegraph transmissions were expensive so those putting together telegraph messages placed a premium on brevity and 'news' was truncated to the bare essentials. Additionally, transmissions were sent from one way-station to the next where one operator had to manually retype the message relayed to the next station, a process that was fraught with error - and was doubly chancy since not all operators at these way-stations spoke English. The net result was that when the news finally arrived it was truncated, error-prone and often bore little resemblance to the initial information that was transmitted.[98]

The Royal Navy found the telegraph to be an important tool in communicating with its global fleet, but that ease and speed of communications came with a price. During times of tension, fleet commanders were often found on their command ships, alongside in port for access to telegraph messages rather than out at sea with their ships.

The speed-up of communications due to the electronic telegraph allowed naval commanders to keep better track of their forces and ongoing events around the world.[99] In 1904 Britain's First Sea Lord, Admiral John Fisher, took advantage of the new technology and developed what noted defence analyst, Norman Friedman calls picture-based warfare.[100] As will be discussed in greater detail in Chapter Three, Admiral Fisher established war rooms to build a tactical picture of where British merchant ships had been attacked by raiding ships. Information collected from the UK's many diplomatic and military stations were fed into two different war rooms - the first tracked ship movements around the world, while the second tracked ship movements in the North Sea. Armed with this picture-based view of the world, Admiral Fisher was able to direct British battlecruisers to locations where British ships were being attacked by raiders.[101] Future British commanders built on Admiral Fisher's successful harnessing of communications technologies to construct a global tactical picture and it served them well in the years leading up to World War I (1914). In the time period between Admiral Fisher's war rooms and World War I, radio technology had matured and was slowly being adopted in Britain as well as in the United States and other countries.

The introduction of the radio revolutionised naval communications.[102] The advent of wireless technology brought the promise of better and speedier communication between headquarters command and fleets at sea. Navies were no longer bound by land-locked telegraph cables, as signals could reach out into the vast expanse of the sea, allowing for central command to better track their forces. This centralised control allowed for better vectoring of fleets based on a centralised information system, but also made it harder for fleet commanders to manage their ships. The first radios used for naval communications used high frequency (HF) waves that provided reliable transmission over long distances, but required very large antennas that were easily detected by the enemy.[103] The success of radio to provide fleet commanders with a timely tactical picture during World War I helped push forward the development of more compact and reliable radio equipment. HF radio remained an important part of the naval communications tool kit as it did very well in long range communications with its ability to broadcast over-the-horizon. However, due to the newness of this technology, naval commanders demanded back-up means of communication, and semaphore and homing pigeons were also used during the early 1900s as a back up in the event of radio failures.[104]

Wireless telegraphs had a huge disadvantage, another 'unintended consequence' of new technology. While wireless technology helped commanders reach far-flung units and communicate in real time, enemy units could also receive these same transmissions and thus gain the tactical advantage over the forces communicating via this wireless technology. History is replete with examples of navies and other forces suffering defeat because the enemy intercepted wireless communications. But clearly, none of this 'downside' was anticipated when the new technology was initially developed and placed on naval units. The Germans learned of the insecurity of HF transmissions during the Battle of Jutland (1916).[105] The British were able to use the information their radio intelligence teams were getting from intercepting German radio signals to steer the fleet to intercept the German High Sea fleet in the North Sea.[106]

By the time of World War II, radio technology had incorporated the use of Very High Frequency (VHF) and Ultra High Frequency (UHF) that allowed for better quality of the transmission of information between ships and between ships and airplanes.[107] The advantage of VHF and UHF signals were that both required smaller antennas and could carry more data that allowed for clear voice conversations and text messages. The disadvantages of the VHF and UHF signals were that their effective range was short - mostly limited to line-of-sight communications - and susceptible to atmospheric disturbances.[108]

Radio technology combined with a successful intelligence gathering apparatus - for example the Pearl Harbor Combat Intelligence Unit - gave the United States a decisive tactical advantage during World War II. The ability of the United States to combine communications technology and intelligence gathering to form a common tactical picture for all commanders to see was evident during the Battle of Midway. Admiral Nimitz was able to anticipate the planned Japanese attack on Midway because the code breakers at the Pacific Fleet Headquarters in Pearl Harbor had intercepted several Japanese communications alluding to the attack.[109] The early warning allowed Admiral Nimitz to organise his fleet and in the battle that followed, US dive bombers were able to catch the Japanese fleet whilst rearming their aircraft. In one decisive action the US carrier forces destroyed the Japanese naval capabilities in the Pacific.[110]

As World War II communications technology advanced, its application brought about changes in what we now refer to as 'command and control', altering the way navy commanders employed their forces. Exploiting the advances in both communications and sensors was a process that had to be learned by naval forces, often at a price. For example, during the naval Battle of Guadalcanal in November 1942, US task force commander Rear Admiral Dan Callaghan found himself overwhelmed by a flood of confusing radar reports over the new 'Talk Between Ships (TBS)' voice radio and his hesitancy cost him the battle and his

life.[111] Communications and the ability to share increasing amounts of information required the commander to revisit both tactics and his role in implementing them. At the same time, the use of advanced communications technology extended the ability of commanders to collaborate and share information, allowing the deliberations of both shore-based headquarters and at-sea tactical commanders to inform and advance tactical decision making. For example, Nicholas Rodger of University of Exeter tells of an incident in 1942 when the commander of the Royal Navy's Home Fleet, Admiral John Tovey, asked the Admiralty to take command of his ships as he had lost track of them while at sea.[112]

Radio remained the chief means of communications through the early part of the Cold War period from the Korean War to the Vietnam War. During the Vietnam War, the US Navy converted small aircraft carriers into radio relay ships to provide reliable radio communications between ship and shore as well as among ships.[113] These radio relay ships and the various radio relay stations established by the US Navy around the world would eventually be replaced by satellites. Satellites, with their persistent line-of-sight capabilities, allowed for the use of Extra High Frequency (EHF) signals at sea.[114] The advantage of EHF signals is that they can carry large amounts of information; voice and data can be carried over the EHF waveform. EHF signals require the receiver to be in line of sight of the broadcaster. Without a relay system - like satellites - to retransmit the EHF signal; ships or other land based receivers that are out of the line of sight would not be able to receive the message. In the years through the Cold War era, satellite transmissions were the main form of naval communications allowing for high tempo manoeuvres at sea and real time coordination between the commanders on shore and at sea.

While the age of steam and electricity revolutionised the way navies communicated, so too did it bring about more lethal and longer range weaponry such as the missile and the 24 hour battle cycle. As noted by naval tactics expert, retired Captain Wayne P Hughes, Jr, US Navy, the modern battlespace that emerged 'will spring more surprises':[115]

> Now, without good scouting, the enemy's missiles can come any time, and with such speed as was never possible under sail and only sometimes possible in World War II. A commander at sea faces a twenty-four-hour war. The night-time Battle of the Nile was an anomaly in 1798. In modern war night action will be commonplace.[116]

Modern Naval Communications

The speed and lethality of the modern battlespace brought about the need for commanders to extend their range of situational awareness through the adoption of the technologies of the computer age. The age of missiles and long-range nuclear weapons refocused attention to improving the speed of weaponry and fires and

scouting or sensing.[117] The increased tempo of the battlespace that came with guided missiles and aircraft forced navies to rethink how better to communicate and gather vital information to assess what was out there.[118]

A telling example of the need for more effective capabilities to meet the jet age emerged in the 1950s when US Navy fleet exercises revealed that Combat Information Centres (CIC) organised around manual and analogue technology had trouble detecting 'enemy' aircraft. The slow pace of detecting, cataloguing enemy and friendly aircraft, and communicating with airborne early warning aircraft quickly overwhelmed the CICs of the fleet. During one exercise in the 1950s conducted by Sixth Fleet:

> The load was so great and communications so slow that half of all bandits [enemy aircraft] closed seventeen nautical miles or more between being detected and having CAP [Combat Air Patrols] assigned. Delays in the arrival of CAP further reduced defence effectiveness, so that in the end, three-quarters of all raids arrived at the force completely unopposed by fighters.[119]

Work began in the United States and in other western navies - particularly in the United Kingdom and Canada - on automating combat systems to improve fleet reaction times to jet age threats. An officer in the Royal Canadian Navy, Lieutenant James Belyea, proposed early on that digital computers could be the key to improving combat systems. Lieutenant Belyea and a Canadian engineer, Stanley F Knights, proposed a digital link that would 'connect the systems aboard ships operating together'.[120] Thus, began the birth of tactical data links and the digital command and control technology that emerged during the Vietnam War era.

The development of tactical data links allowed the almost instantaneous sharing of sensor data between ships and aircraft, and provided commanders a common view of force sensors and the ability to rapidly coordinate operations. Tactical data links and computerisation proved to be invaluable assets to the US Navy during operations in the waters and airspace of North Vietnam. Naval Tactical Data Systems (NTDS) along with UHF radio systems made it possible for the US Navy to network their ships and aircraft with each other and with the US Air Force. This early 'netting' of assets allowed the US fleet to obtain an operational picture deep into North Vietnam to counter the North Vietnamese MiG threat.[121]

The development of ARPANET[122] and its growth in the 1970s began the Information Age, where fast evolving computers were connected to grow the World Wide Web, now known as the Internet.[123] While the Internet spurred an information and communications revolution in the private sector, another revolution was being discussed among defence scholars and thinkers.

The Revolution in Military Affairs (RMA), begun in the Soviet Union, entered into the lexicon of US military thinkers. RMA was first brought forth by the Soviets in the 1940s and argued 'that the combination of nuclear weapons, jet aircraft, and missiles had drastically changed warfare…[and] computers (which they called cybernetics) would have a similar impact'.[124]

Within US defence circles a primary concern was how to conduct force planning after the fall of the Soviet Union and the emerging era of smaller defence budgets. Military and civilian defence planners struggled to devise the proper force construct to manage the United States' new position as the global leader, yet work with fewer battalions and ships. For example, the US Navy, at the height of the Cold War, boasted a fleet of over 590 ships. When the Soviet Union collapsed and the Cold War ebbed, the US Navy's fleet shrunk dramatically to 392 in 1995 and to the current level of around 280 ships.[125]

It was in this environment of balancing that the US military's increased engagement in 'operations other than war' (OOTW) and decreasing force structure that military leaders and strategists examined the promise of information communication technologies (ICT) and netting as a means to do more with less. General Gordon R Sullivan, US Army Chief of Staff from 1991-95, was an early proponent of the US RMA discussions and the use of computer technology to transform the way wars are conducted by 'increasing the lethality of modern armies not geometrically, but exponentially'.[126] In a 1993 Army Strategic Studies Institute publication, General Sullivan and his co-author Lieutenant Colonel Dubik argued that:

> Integrative technologies will enhance the ability of commanders and their units to fight with scarce assets. The complete use of integrative technologies will revolutionize command and staff procedures. Software will allow much of the information now transmitted by radio and synchronized on acetate and charts to be self-synchronized automatically, computer-to-computer. Smart command and control systems will create a common perception of the battlefield and the theatre among members of a joint task force.[127]

In the years since the US Army's integrative technologies concept was introduced, several additional concepts entered into the lexicon of military strategic thought and planning. Some, like the dominant battlespace concept, introduced in 1995 in a National Defense University publication, expanded the US Army's integrative technologies to an overarching concept for the general force. The dominant battlespace concept was defined by Admiral William Owens as a new 'systems of systems' concept:

> Merging our increasing capacity to gather real-time, all-weather information continuously with our increasing capacity to process

> and make sense of this voluminous data builds the realm of dominant battlespace knowledge (DBK). DBK involves everything from automated target recognition to knowledge of an opponent's operational scheme and the networks relied on to pursue that scheme.[128]

The ideas professed by RMA thinkers like General Sullivan and Admiral Owens to use information age technologies to revolutionise the way the United States wages war were documented officially in the 1997 *Quadrennial Defense Review* (QDR). The QDR is a congressionally mandated review of the US military to provide the civilian leadership and the American public an assessment of the Defense Department's strategies and priorities. The first QDR was produced in 1997 and set the United States military on the course to transforming to achieve 'information superiority':

> The ongoing transformation of our military capabilities - the so-called Revolution in Military Affairs (RMA) - centres on developing the improved information and command and control capabilities needed to significantly enhance joint operations. With the support of an advanced command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) common backbone, the United States will be able to respond rapidly to any conflict; warfighters will be able to dominate any situation; and day-to-day operations will be optimized with accurate, timely, and secure information. Just as much of the non-defence world has become increasingly interconnected through the growth of internetted communications, the Department of Defense is working to provide a complementary, secure, open C4ISR network architecture.[129]

Out of the RMA discussions in the US Department of Defense (US DoD) and the military services, emerged the Network-Centric Warfare (NCW) concept - the current working vision of building a C4ISR capability that would transform military capabilities. Previous works on force transformation - such as the Army's integrative technologies and the National Defense University's dominant battlespace awareness concepts - provided a generalised concept of the need for military transformation but did not have the necessary real-world examples to support the theory.[130]

Introduced to the defence community in 1998 by Vice Admiral Arthur Cebrowski and John Garstka, NCW was developed to take advantage of information and communications technologies and business processes that were changing how businesses operated.[131] The authors pointed to several businesses like Walmart that had used information and communications technologies to keep detailed reports on the levels of inventory that was shared directly with vendors who could

better determine what was needed at various Walmart stores.[132] Cebrowski and Garstka argued in their US Naval Institute's *Proceedings* article that successful businesses employed:

> …network-centric operational architectures that…provide the ability to generate and sustain very high levels of competitive space awareness, which is translated into competitive advantage.[133]

For the United States military to be successful and move away from attrition warfare towards the more complex and varied missions contemporary operations call for, it had to harness the network-centric concept that would promote a 'bottoms-up', self-synchronising organisational model.[134] The NCW concept became the US DoD's way forward when Admiral Cebrowski became the director of its Office of Force Transformation in 2001. NCW was defined and elaborated for the military services in a series of publications by the US DoD's Command and Control Research Program (CCRP):

> The term, NCW, provides a useful shorthand for describing a broad class of approaches to military operations that are enabled by the networking of the force. 'Networking the Force' entails much more than providing connectivity among force components in the physical domain. It involves the development of doctrine and associated tactics, techniques, and procedures that enable a force to develop and leverage an information advantage to increase combat power.[135]

The application of NCW to the modernisation of not only the US Navy's C4ISR systems but other navies as well will be covered in the following chapters but, in short, the modern United States military is working to net not only individual forces but also the joint force.

Adopting a networking concept has been the goal of not only the United States military modernisation efforts but also of other nations, including the ADF and their implementation of NCW. The Australian Defence White Paper, 2009, notes the importance of networking the force.

> The future ADF will use modern information technology to link sensors, weapons systems and commanders and their personnel in a networked environment. This will help our people to work more effectively together, provide common battlespace awareness and, most crucially, information superiority over an adversary so that our people can make critical decisions on the battlefield more quickly and with better knowledge than the adversary. This approach will be dependent on a secure high-capacity information network that allows personnel located in different areas to collaborate in real time, and to synchronise their operational actions very precisely.[136]

Australian Maritime Doctrine builds on the notion of the power of networking by noting that it has increased the reach and utility of the naval force. It notes that 'force networking systems' have allowed 'warships to better "view" and intervene in the land, air and land-air-battles by integrating the activities of all units involved'.[137] At the centre of this force networking system are the advancements in technologies that have sped up the flow of information:

> Developments in *data links* and satellite communications have increased the speed with which information can be transferred to the commander and individual units...This has improved their awareness of the battlespace and their ability to operate within it. Furthermore, networking developments are increasing the ability of all units to contribute to the achievement of battlespace awareness.[138]

Communicating at sea, with the aim to better understand 'what is over that horizon', as well as coordinate operations, has been a major endeavour for navies for millennia. To gain a better picture of the situation, navies have led the integration of the latest information and communications technologies into their operations. These information and communications technologies have taken various forms since the dawn of warfare - from signal flags to the harnessing of radio waves to networking communications technologies together in the digital age.

For medium sized navies like the RAN, the ability to network not only within the service but with a joint force has helped to bridge some crucial gaps such as maritime air warfare. As the RAN operates without its own carrier and fixed wing maritime combat air capabilities, networking allows naval forces to integrate with the 'air component of the joint force' to ensure sea control.[139] However, as the RAN works to build its networking capabilities with a joint force, it must also work to ensure that it can operate with coalition partners who are also networked such as the US Navy. The following chapters will delve into the efforts of modern day navies to net together as it is no longer enough merely to communicate at sea but navies must now 'network' to fight effectively.

3. Communications Evolves into Networking

Technological Advances Enable Navies to 'Push the Edge' of the Information Envelope

Throughout history, navies have been at the forefront of 'pushing the edge' of the information envelope and evolving methods to communicate and network at sea. This is intuitive because armies have, until only recently, typically fought in concentrated areas where communications between supporting units could often be as rudimentary as a soldier running between units to carry a command or a friendly unit observing an enemy force through binoculars.

Navies, on the other hand, have most typically been dispersed over wider-and-wider distances. As Dr Norman Friedman points out in *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars*, '[t]his kind of warfare came to navies first because they dealt with wide areas in which relatively small forces were dispersed. It is only now coming to armies that deal with large numbers packed into limited areas'.[140]

The fact that navies have been leaders in developing networking technologies has been well-documented in a wide array of publications and studies, most notably previous publications - and especially conference proceedings - published by the Sea Power Centre - Australia, as well as notable books and publications by various 'think tanks' throughout the world.

In the latter part of the twentieth century, the US Navy, reflecting its traditional style of operations, which entailed the continuous forward deployment of a distributed force far from US territory, or supporting infrastructure, developed the concept of networking to ensure timely and reliable communications links to ensure the most effective employment of scattered forces. As early as the 1960s, the US Navy was experimenting with the Tactical Data Information Exchange System (TADIXS), which was the progenitor of the tactical data systems such as Link 11 shared by many navies today.

Armed with increasingly reliable tactical data links, global navies began to recognise the potential of this ability to link ships at vast distances to revolutionise naval warfare. As Dr Loren Thompson points out in *Networking the Navy: A Model for Modern Warfare*, many of the concepts driving the networking of military forces today began to evolve two decades ago:

> In 1990, long before network-centric warfare became a central feature of joint doctrine, the [US] Navy established a program called

> 'Copernicus' to assimilate emerging information technologies… The admirals managing Copernicus understood that information technologies had the potential to revolutionize naval operations. The Navy adopted the phrase 'network-centric warfare' to describe this nascent warfighting paradigm, because it stressed integration and communications over autonomy in conducting naval operations.[141]

Over time, Copernicus evolved into what the US Navy called 'IT-21'. As pointed out by Admiral Archie Clemins, then-commander of the US Pacific Fleet, in a ground-breaking article in *CHIPS* magazine in 1997,

> IT-21 is a reprioritization of existing C4I programs of record focused on accelerating the transition of a PC-based tactical and support warfighting network…The goal of IT-21 is to link all US forces and eventually even our allies together in a network that enables voice, video and data transmissions from a single desktop PC.[142]

The following year, Cebrowski and Garstka built on Copernicus and IT-21 to envision war fighting in the twenty-first century. Their 1998 US Naval Institute *Proceedings* article, 'Network-Centric Warfare: It's Origin and Future', described the potential of network-centric concepts to alter the nature of warfare itself, moving decisively from 'platform-centric warfare' to 'network-centric warfare'. Although published well over a decade ago, their vision of network-centric warfare proved remarkably prescient:

> Network-Centric Warfare derives its power from the strong networking of a well-informed but geographically dispersed force. The enabling elements are a high-performance information grid, access to all appropriate information sources, weapons reach and manoeuvre with precision and speed of response, value-adding command and control (C2) processes - to include high-speed automated assignment of resources to need - and integrated sensor grids closely coupled in time to shooters and C2 processes. Network-centric warfare is applicable to all levels of warfare and contributes to the coalescence of strategy, operations, and tactics. It is transparent to mission, force size and composition, and geography.[143]

Theory met reality in the early part of the twenty-first century, when the United States, in response to the terrorist attacks of 11 September 2001, launched Operation ENDURING FREEDOM (OEF) to attack terrorist strongholds in Afghanistan. The ensuing campaign vindicated what the proponents of network-centric warfare had been advocating all along. As CNO Admiral Vern Clark pointed out regarding the US Navy's experience in OEF; '[e]ighty percent of the Navy strike sorties attacked targets that were unknown to the aircrews when they left the carriers. They relied

upon networked sensors and joint communications to swiftly respond to targets of opportunity'.[144]

Admiral Clark evolved a vision for the US Navy called *Sea Power 21: Operational Concepts for a New Era*.[145] Some critics described the three pillars of Sea Power 21 (Sea Strike, Sea Shield, and Sea Basing) as 'old wine in new bottles', but Admiral Clark also introduced a new term, FORCEnet. Admiral Clark described FORCEnet as 'an initiative to tie together naval, joint and national information grids to achieve unprecedented situational awareness and knowledge management'.[146] While new to some, FORCEnet was clearly the next step in the evolution of the Navy's networking capabilities.

Loren Thompson points out that; 'FORCEnet was the greatest system-integration challenge ever proposed in the history of warfare'.[147] Regardless of whether this is true or not, the US Navy made an enormous capital investment in FORCEnet and in the wide array of programs that instantiate the network-centric warfare concept.[148] While the term FORCEnet has receded from everyday use, the concepts associated with it - netted forces afloat and ashore - remain as a part of the US Navy's modernisation efforts. The investments put in place as part of the early FORCEnet initiatives have the potential to provide navies united in global or regional maritime partnerships with a ready-made infrastructure to leverage and support their networking efforts. In Chapter Five we will elaborate on this further when discuss our 'Beta Test' and analysis.

As discussed in Chapter Two, many modern navies have been innovators in adapting extant technologies to serve the unique needs of the maritime environment and in creating new technologies specifically tailored to naval needs. The old saw 'necessity is the mother of invention' is especially apt in describing how navies have evolved their communications systems over the centuries. Technological advances - particularly within the past several decades - have fundamentally transformed the way navies operate at sea to address maritime security challenges.

As navies began to operate at increasingly vast distances, they soon needed to rapidly adapt modern communications technologies. The new technologies were typically those classified as command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) technologies. Once generally categorised as 'enablers' of other technologies - sensors, systems and weapons - C4ISR technologies are now considered as weapons - often as *the* weapon of choice. As nations and navies continue working together to address maritime security challenges in the global commons, the navies of virtually all nations have embraced new naval C4ISR technologies and inserted them into their naval ships, submarines, craft, aircraft and command centres in order to provide their navies with the technological 'edge' at sea.

The need for effective C4ISR systems for the RAN - as well as other navies the RAN will likely partner with - was highlighted in the *Future Maritime Operating Concept - 2025: Maritime Force Projection and Control*, which noted:

> The effectiveness of the maritime force can be improved through information and decision superiority [quantity and speed]…C2 systems must be able to deliver superior battlespace awareness and management through decision speed and quality thus controlling operational tempo…The maritime force must also develop a high level of interoperability with likely coalition maritime forces and future architectures must provide a cohesive and comprehensive system through NCW [network centric warfare] to achieve complete battlespace awareness and control.[149]

But as C4ISR technologies have advanced over the past several decades, they have dramatically enhanced the ability of navies to not only communicate, but to 'network' vast amounts of data and information at increasing speed, often over vast distances. This ability to network has ushered in heretofore-unknown capabilities and has enabled navies to push the edge of the information envelope and evolve the 'art of the possible' at sea.

'Networking' Supplants Communicating for Modern Navies

Today, no modern navy will put to sea without its C4ISR systems at a high level of readiness. In much the same way that C4ISR technologies themselves are now viewed as weapons, a naval force at sea unable to network will not only be unable to complete even the most rudimentary missions, but will also be virtually defenceless against a modern foe. It is not an overstatement to say that C4ISR systems have become the *sine qua non* of success for modern navies.

New C4ISR technologies have had a profound and positive impact on the ability of navies to network their own ships, submarines, craft, aircraft and command centres, and to freely and seamlessly exchange data and information within each navy. And navies have found, conclusively, that their effectiveness is directly proportional to their ability to not only communicate, but to network, both at sea and ashore. Because of this, every modern navy has sought to install networking technologies - often as rapidly as they can afford them.

This need to have a 'networked navy' is recognised at the highest level of most defence establishments. Indeed, the 2009 Australian Defence White Paper puts the requirement to have a networked force this way:

> Defence requires a fully integrated command support system covering all levels of operation and all environments, with the ability to participate in coalition operations…To take maximum advantage of the suite of sensors, weapons and other systems that are being acquired, Defence needs to ensure that it adheres to a centrally coordinated plan to link those elements together in what will over time become the networked force.[150]

This imperative is not limited only to the Australian government as other defence establishments have also been 'on record' regarding the importance of having a networked force. For example, the Canadian strategic publication *Landmark - The Navy's Strategy for 2020* puts it this way:

> Success in optimising [C4ISR technologies] will be perhaps the single most important capability that will allow Canadian naval forces to provide viable support to national and multinational objectives … With the clearly established objectives in *Strategy 2020* for greater interoperability and modernization, a guiding principle of future force development will be achieving 'seamless operational integration at short notice,' with our major allies (and the USN, in particular), in these key areas of warfare.[151]

A continent away, British Major General John Kiszely was quoted in the *RUSI Journal* putting the imperative this way; '[f]ull interoperability between forces would depend upon integrated collaborative planning based on the maintenance of a common operating picture and common intelligence inputs. Without appropriate digital communications, this would not be practicable'.[152]

International journals in many nations - especially Commonwealth nations - have continued to emphasise the importance of networking as a bedrock requirement for effective warfighting. And this bedrock requirement is increasingly important among nations. NATO's 2010 vision document, *NATO 2020: Assured Security: Dynamic Engagement,* puts C4ISR capabilities squarely as a transformational capability. The document notes that the conflicts in Kosovo and Afghanistan have demonstrated and underscored the need for interoperable command and control capabilities between and among NATO partner nations, noting in particular:

> C4ISR capabilities provide the operational sinew binding NATO and national forces together into an interoperable, agile and cohesive whole. They should be a high priority for future investment by members as well as by NATO itself. Allies should invest first in compliance with the latest NATO CIS architecture and ISR platform standards. Likewise, NATO should ensure the same architectural standards are met and maintained across its command structure.

> Allies and partners should emphasize investment in national systems at the tactical and operational levels that will tie into NATO's strategic-operational networks.[153]

Clearly, there is general recognition within and among navies large and small that the ability to network at sea is a critical capability and projects like NATO's Network Enabled Capability (NNEC) are designed to enhance coalition networking. But with defence budgets in most nations constrained - often severely - the question of what networks deliver must be addressed in order to ensure appropriate funding levels.

Networks Deliver a Superior Tactical Picture

If there is a consistent 'theme' in the ongoing quest for navies to network more effectively, it is to enable these networks to ultimately deliver superior situational awareness to decision-makers to enable them to make better and faster decisions than the enemy can. In a paper delivered at the RAN Sea Power Conference 2006, Dr Norman Friedman put it this way:

> A reasonably persuasive theory of combat holds that the enemy's will can be destroyed if he cannot move quickly enough to react to successive blows. In this 'OODA loop' theory, combat is cyclical, consisting of observation, orientation, decision and action. If the cycle used by one combatant is significantly slower, the combatant loses the ability to understand what is happening to him; ultimately he suffers what amounts to a nervous collapse. OODA loops success can be achieved by a combination of accelerating our own operations and slowing the enemy's.[154]

In order to fully understand the entire issue of networking and navies, it is important to recognise that, despite what some proponents of networking would have us believe, this notion of networking and developing a tactical superior picture to warfighters is not new. In fact, it is over a century old, and understanding this is imperative to examining how navies can achieve better networking in the future. Spurred by the British success in World War I, throughout the ensuing century, nations and navies have built on Admiral Fisher's notion of 'picture-based warfare' to develop better intelligence sources, better networking, and most importantly, a better tactical picture. Admiral Fisher was able to get inside the 'OODA loops' of potential enemies using the best 'all-source intelligence' available. No nation has had the upper-hand in winning the 'picture-based-war' to the extent Britain did during World War I, although the record points conclusively to the fact that nations such as the United States, Russia, Britain, Germany and Japan involved in major conflicts through the century invented and innovated most rapidly to advance the state of picture-based network-centric warfare.[155] If the history of warfare over the past century - where nations and navies evolved better networks and better

pictures to defeat foes - has taught us anything, it is that effectively networked command and control links and a useful tactical, operational and strategic picture have made it possible for navies especially to fight in a new way. And the data is compelling that if one side uses a networked approach, it can gain decisive advantage over an enemy.

C4ISR Technologies Continue to Evolve Rapidly and Expand the 'Art of the Possible' for Networking

C4ISR technologies are developing at an extraordinary pace, so much so that nations and navies have found it important to keep abreast of the absolutely latest developments in the field of information technology (IT). Part of this process is working to determine just how these technologies are evolving. This section represents our work to determine the trajectory of these trend lines and present a vision of the future capabilities that C4ISR systems may provide.

US Navy's Space and Naval Warfare Systems Command (SPAWAR), the US Navy acquisition command charged with acquiring naval, joint, intelligence, national, IT, space, and enterprise systems, provides a well-nuanced view of the future of C4ISR in their vision document, *Naval IT, C4ISR, Space Systems, and Enterprise Support: Today and Tomorrow*, where it notes:

> Operations in the maritime domain demand Command, Control, Communications, and Computers (C4) capabilities both globally and regionally coupled with Intelligence, Surveillance, and Reconnaissance (ISR) assets. For enhanced maritime capability, services must exploit new military technologies and capabilities among regional allies. At a minimum U.S. forces and allies must share common C2, with regular participation of coalition officers trained to work on combined staffs. When these prerequisites are met, the integration of compatible C4ISR systems for warfighter decision-makers becomes a coalition force multiplier, enabling effective integration of US capabilities with allies - a true collaborative environment for military operations.[156]

While C4ISR technologies have been advancing rapidly in the commercial sector, these new technologies have been applied to militaries somewhat more slowly. This is because the disciplined, methodical approach of most military acquisition organisations does not easily lend itself to rapid, large-scale technological insertion. In fact, the US DoD Defense Science Board concluded that 'the conventional DOD acquisition process is too long and too cumbersome to fit the needs of the many IT systems that require continuous changes and upgrades'.[157]

Despite this challenge, however, these technologies *are* beginning to change the ways that militaries - and especially naval units - organise and fight.

Today, C4ISR tools are principally designed to support a focus on kinetic warfare. This is not to say that militaries - and especially the US military - do not recognise, and are not organising to deal with 'cyberspace', because clearly they have. At the DoD level, the creation of a US Cyber Command (USCYBERCOM) was announced in June 2009. Additionally, the Navy has successfully followed suit by standing up its own Fleet Cyber Command, which was activated on 29 January 2010. Similarly, the Australian Cyber Security Operations Centre was officially opened on 15 January 2010, as an early outcome from the strategic vision established in the 2009 Defence White Paper. However, these are quite recent phenomena.

As mentioned above, militaries and navies rely on C4ISR technologies to conduct kinetic operations. However, the value of these technologies is hampered to the extent that their users often fight in a way that only loosely connects planning, situational awareness and execution. All too often, these functions are still conducted in a somewhat 'stove-piped' manner that does not lend itself to a robust continuum where one function flows into the other using the same tools and techniques. While some progress has already been made, clearly it is one area that is ripe for further innovation and technological improvement.

The technological solution with the most promise of integrating these functions is the real progress made in the migration of stove-piped applications into a more network-centric, services-oriented architecture (SOA) environment. The US Navy's work in this area has progressed substantially and the US Navy's next generation afloat and ashore network infrastructure acquisition efforts - Consolidated Afloat Networks and Enterprise Services (CANES) and Next Generation Enterprise Network (NGEN) - both specify requirements in terms of the services to be provided.[158] This approach also starts to drive systems to realise the benefits of SOA by characterising the system in terms of services. These service-level requirements are often more detailed than traditional functional requirements, and by identifying common services one can begin the task of reusing them across business processes or mission threads.

One unique naval challenge that continues to impede progress on C4ISR technologies is the problem of limited bandwidth at sea. Unlike units ashore, information 'pipes' to and from naval vessels are limited - often severely in the case of smaller ships, submarines and other vessels - and while good work is being done today, this remains a challenge that is just beginning to be addressed. Compounding this bandwidth issue is that as the amount of data increases, the effective throughput of ever-stressed wireless data links continues to decrease. This creates an untenable situation, particularly during times of high operational tempo, and much work is needed to de-conflict this congested spectrum.

Another challenge - not unique to naval units, but clearly more pronounced than for land units - is that of security. Just as the Victorians discovered a huge downside when *enemy* units intercepted their wireless radio transmissions, naval units today are still challenged with maintaining the security of transmissions between ships at sea, as well as with other units and command centres ashore. Although progress has been made, 'securing the net' remains one of the most severe cyber-challenges.

In short, C4ISR and networking technologies are overcoming the challenges of stove-piped structures and processes, bandwidth restrictions, and security concerns to enable vast amounts of data to be provided to and acted on by naval units. Even so, this is not without its own downside and unintended consequence - that of correlating and fusing these vast amounts of data. While some progress has been made, data fusion, like security, is an area where much work remains to be done.

The foregoing discussion makes clear why, as navies continue to seek the tactical edge, C4ISR technologies will very likely continue to evolve rapidly and shape naval warfare in the future. At that future point the technical community in Australia, the US and the other AUSCANNZUKUS nations will finally have figured out how to filter the data to keep from overloading users. Most importantly, the operator, not the technologist will build the picture he or she needs to meet the mission at hand. Operational users will be able to 'compose' applications and services from multiple sources. For key users this will give them the ability to compose their own mission specific solutions - pick data sources, processing steps and display tools - while less advanced users or those standing a normal watch in a well-defined mission area get a standard 'design time' solution that fits their needs.

C4ISR advances will not only benefit so-called 'high-end' navies, but any navy investing in naval C4ISR technologies can gain a tactical edge. As pointed out by Dr Paul Mitchell in the *Naval War College Review:*

> Network-centric warfare aims at increasing the efficiency of the transfer of maritime information among participating units (or nodes). By optimizing the efficiency of operations through information exchange, often-small naval formations can generate additional combat power. Data is *(sic)* manipulated by a series of dynamic and interlinked 'grids:' sensor grids that gather the data; information grids that fuse and process it *(sic)* and engagement grids manage the operations generated.[159]

As C4ISR technologies evolve along the most likely paths we envision, C4ISR will be truly joint, with common core services and architectures and where solutions are tailored for the platform and mission. This represents a sea change

and transformation, where solutions are tailored for the platform (for example, a command centre, ship, aircraft, or tank) and mission, not the colour of the uniform. We envision an evolving end state where there is effectively a library of capability modules that can be combined in any way the user desires. This will be enabled by whatever technical solutions follow what is currently called services oriented architectures, common data standards, normalised lexicons and the like, and will ultimately result in a true plug-and-play solution set just like Lego blocks.

Unlike today where most planning and execution is focused on kinetic warfare - primarily strike warfare - in tomorrow's hybrid warfare environment the C4ISR systems and services provided will have to be adaptable across the entire spectrum of conflict in peace and in war. This is important because emerging domains like cyber and humanitarian assistance do not fit well into current tools and processes. The C4ISR tools of tomorrow will be adaptable across a wide array of missions and scenarios, and will often be used to simultaneously support multiple types of missions.

In 2030, we envision a future state of C4ISR where information is truly and completely platform agnostic.[160] Users will have a few common client applications that consume almost anything and will have other, smaller, focused applications that do one very explicit function. As C4ISR evolves over the next two decades we envision a world where we build fewer - but more capable - data presentation tools. In the decades hence, common data formats, good metadata and flexible display tools will allow the user to pick any field of information and vary the display based on that - dynamically filtering the data to facilitate understanding and decision making. We envision this as a fuller maturation of today's technologies such as Google Earth and other cutting-edge applications.

One of the most important - and beneficial - trends we see accelerating is the use of automated workflows to help guide operators through often-complex C4ISR processes and the widespread use of agent software to automate routine tasks, especially those that are time-consuming and not needing constant human intervention. In this future state, workflows plus agents will be the key in dealing with - and indeed overcoming - information overload. This is crucial especially in a high-stress warfighting environment where having a library of predefined workflows allows even a novice user to perform at an acceptable level by leading them through the process. Agents attached to the workflow do the heavy lifting by gathering and filtering data. As we evolve to this end state we envision operators 'training' their web-enabled personal assistants to perform myriad tasks, even performing tasks like determining what meetings and whose email is important to this user so the agent can assist the user in time management.

As one small example of how these workflows and agents assist the operator (read 'watchstander' in this case), consider the case of maritime domain awareness

(MDA), a core requirement for effective operations at sea in any scenario along the spectrum of conflict. In the future, a new operator will be assigned to stand an MDA watch. That operator will log into portal and select the MDA tab. The automated workflow will bring up a map with maritime vessel Automatic Identification System (AIS) data, but this data is voluminous and in most cases is far more than is wanted or needed and does nothing to inform the watchstander.[161]

In this future state of C4ISR, the information overflow of AIS data will be tamed by data agents that will filter and manage the information. For instance, a maritime motion model agent can be used to filter out tracks behaving as expected - those tracks that the user need not be concerned with. Other agents can then be employed to look for inconsistencies in AIS data, in other words, those tracks 'behaving oddly' and which merit possible intervention and investigation as assigned by a human operator. If the operator determines that a particular track merits further investigation, he or she will use other agents to help operators assign tasking to resources to look at tracks that require further investigation.

In 2030, as C4ISR evolves, we envision a world where a combination of agents and better data visualisation tools leads to better filters on what information is delivered and displayed. At this future point we will use agents - small focused applications that will tirelessly do the same thing 24/7 - that are trained to do myriad tasks. For example, future common operating pictures can be adjusted to meet the demands of different users, we recognise that not all users need or want the same picture. Therefore, in the future, agents can be used to automatically adjust the level of information, and even the format it is delivered in, to reflect the differing needs (and available bandwidth) of the decision maker - whether they are at the operational or tactical level.

In much the same way as these trained agents work around the clock to tailor information to various levels of command, they can be trained to alert operators to important tactical, operational, or strategic events. For example, agents will watch a trip line or exclusion zone day after day without getting tired and you can have hundreds or thousands of them looking for all sorts of indicators you want to be alerted to. These sorts of functions are just beginning to find their way into various command centres, but we envision their use will explode in the coming decades.

Today, even in scenarios where an enemy is not trying to thwart our efforts through cyber attacks, bandwidth constraints are a constant factor at the tactical, operational, and strategic levels. In decades hence, it is all-but-certain we will have adversaries that can adversely impact our communications via cyber and other attacks. Agents will be able to detect a loss in available bandwidth and will automatically prioritise what traffic goes over what network, throttling down applications that can deal with less data and putting up bulk updates and large file transfers.

By 2030 we envision a state where advances in visualisation tools and correlation and fusion approaches will yield a seamless, multi-spectral, augmented-reality view of the world tailored to each user. At this future point, all data will be fused and available in single map-based client. We will have met the challenge of how to include and how to combine and present data (for example, video) from multiple data sources. We will be able to present multi-spectral data that the human eye cannot see and we will find ways to present information so we will not overwhelm the user with textual information for the objects in their field of view.

Led by the demands of operational users in the current conflicts in Iraq and Afghanistan, the use of unmanned or autonomous systems has exploded and commanders at every level literally cannot get enough of them. Autonomous vehicles participate in every mission - as a scout, a local eye in the sky, as a communications relay or, in some cases, as the actual weapon platform for a strike. Today autonomous vehicles are used in *every* type of mission and as technology advances they will generate increasingly voluminous streams of information. However, this state-of-the-art practice has had unintended consequences. First, the volume of data these autonomous systems generate currently defy attempts to process, fuse, and analyse the data - it literally overwhelms the operators and tremendous amounts of data are simply discarded. Likewise, the term 'unmanned' is a complete misnomer, for these *autonomous* systems often require multiple operators on virtually every mission.[162]

That said, autonomous systems are used more frequently today and we envision that in the future these systems - air, ground, surface and subsurface - will have evolved to the state the data they generate will be fused and provided to operators via a discrete number of pipes, versus today's paradigm of each autonomous system passing its data along a single pipe to a single receiving station. Even more significant breakthroughs will occur that will completely eliminate today's paradigm of 'one operator, one joystick, one unmanned system'. This sea change is being driven by two significant factors; the rapidly increasing cost of military manpower, costs that far exceed all other costs of military systems, and the need, especially in the naval context, to reduce the numbers of sailors on ships. Breakthrough work in areas such as the UV-Sentry program and the Multi-Robot Operator Control Unit (MOCU) offer a clear road ahead to this future state.[163]

MOCU is a project that offers perhaps the most promising glimpse into the future of autonomous systems. It is a groundbreaking unmanned project that directly addresses the challenge of allowing one operator to control multiple systems in order to reduce manning costs. MOCU is a graphical operator-control software package that allows simultaneous control of multiple heterogeneous unmanned systems from a single console. It has been designed to address interoperability, standardisation, and customisation issues by using a modular, scalable, and

flexible architecture. To date, this software has been used in multiple platforms, including being integrated into the US Navy's Littoral Combat Ship (LCS) program for both the Mine Warfare and Anti-Submarine Warfare (ASW) missions. A third-generation product, based upon a publish/subscribe architecture, is currently under development.[164] This update completely decouples the human interface from the core management software, thus allowing even more flexibility in user customisation of the product.

As hybrid warfare makes military planning more complex, the ability of human operators alone - even legions of them - to effectively plan a military operation is under increasing stress. And once an operation is under way, the ability of these operators to observe a perturbation in a plan, react to it, and establish viable alternatives at very short notice is almost totally absent in our militaries today.

But with the C4ISR systems of the future we envision a state where operators using state-of-the-art planning systems will be able to evolve their situational awareness to a place where they can focus on effects delivered, not just platforms. And because planning will be done online, the systems will know in fine detail who should be where, when; and agents can monitor the execution of a plan, and alert the operator when there is an event that interferes with the plan. This could be, for example, a logistics aircraft with critical parts or personnel, experiencing a mechanical problem and not arriving where it is expected on time. Today, when a perturbation in such a plan occurs, staff members are hastily assembled to review the situation, develop alternatives, brief the commander, and then determine a course of action. But as the pace of warfare accelerates, this option is becoming increasingly unsatisfactory. As the state of C4ISR evolves over the next decades, we will reach a state where agents begin to look at the operational impact the moment a perturbation occurs and devise a series of options with pros and cons. Critically, modelling and simulation must be available to every user and be a seamless ever-present element of the planning process.

In the early 2000s only information operations practitioners and intelligence analysts worried about the relationships between people and between computers as well as between power distribution systems and the inter-relations among those networks. As C4ISR evolves in the next two decades, we will see greater emphasis on understanding networks (social, economic, computer, power, and others). We will have evolved to a state where warfighters will be able to recognise the elemental importance of networks of all kinds to every type of warfare and where they have the data and tools to support this key type of analysis.

Advanced user-interfaces are evolving to a point where the stuff of fantasy just a few years ago is fast becoming reality. The user-interface future where everything supports touch, useable voice recognition and computer vision has been realised with multi-touch interfaces available on every device. In addition, users can interact

with computers via voice control and speech output and computers are more aware of their environment through computer vision systems.

Taking advantage of currently evolving technologies, in the decades hence we envision a world where virtual reality has become indistinguishable from actual reality - in fact it will be better because we can add additional data that you cannot see in the 'real' world. In other words, 'augmented reality' will be what every operator will expect. Put another way, all tactical forces will have heads-up displays, not just the fighter pilots. We may even have evolved to the state where the lowest tactical-level user will have some version of direct neural interface, 3D projectors, and very large, flexible displays.

Finally - and in some ways most importantly - we see a dramatic change in the way we will secure the information that is generated by a plethora of sensors, transported via a variety of networks, and processed, analysed and displayed on a wide array of command and control systems. Events like China's hacking of Google servers in 2010 brought worldwide attention to both the vulnerability of even the most secure networks and the determination of some to invade the networks of others.[165]

We envision a world in the not too distant future where we will be able to control data at the field level - and down to packet level in transit - control who can see it, determine if it arrived intact, and if not, then find out who touched it. This ability to tag data at the field level, and to trust that those tags have not been tampered with is key, since it enables not only the agents to help with filtering data but also finally makes cross-domain and multi-level security problems solvable. As we do this over the next two decades, packet level encryption and multi-path routing will largely solve the bandwidth problem since they allow the use of any communications channel available - even the enemy's - and will enable a whole new business of third parties who will launch communications satellites for lease back to us.

This view of the future of C4ISR presented above helps us to understand *why* navies have been so aggressive in pushing the edge of the technology envelope against potential rivals in the naval and joint warfighting environment of the future. But as this technology infusion has occurred, it has brought challenges as well as opportunities.

Modern Navies have Aggressively Pursued Networking Technology Infusion

While every navy is ultimately constrained in what it can buy by budgetary considerations, the refusal of most navies to surrender the C4ISR technical and tactical edge to adversaries has led to a pronounced increase in spending on these systems. Coupled with the increasing (some would say spiralling) cost

of ships and aircraft, nations and navies often find that an investment in C4ISR technologies offers the best return on investment.

Clearly, the type of navy a nation acquires has an enormous impact on how aggressively it intends to pursue networking technologies. For the ADF in general and the RAN specifically, there is compelling evidence that Australia will be a leader in building a navy equipped for high-end, coalition warfare that will demand acquisition of robust C4ISR systems. As Commodore Jack McCaffrie (ret) and Dr Chris Rahman point out in the *Naval War College Review:*

> Recent, ongoing, and future (Force 2030) ADF capability developments will dramatically enhance the potential for Australian maritime forces to contribute to U.S.-led coalitions in future contingencies. The air warfare destroyers and, especially the new frigates – with their LACMs, SM-6 missiles, CEC, possibly theatre-ballistic-missile defence, and advanced antisubmarine warfare systems – would add measurably to any US Navy-led maritime force…The white paper proposes a robust future defence force with a very strong maritime emphasis, including a sea-based strike capacity and the ability to deploy, protect, and sustain a substantial land force.[166]

As mentioned earlier, these new C4ISR technologies have had a dramatic impact on the ability of many navies to network with their own ships, submarines, craft, aircraft and command centres. This has led to a situation where various naval components can exchange vast amounts of information *within* each navy. As they have done this, these navies have found that they become more effective across the spectrum of conflict, from peacemaking, to counter-insurgency, to major conflicts. However, this rush to install the latest cutting-edge technology in each navy has had just the *opposite* effect on the ability of navies to network effectively between and among the ships, submarines, craft, aircraft and command centres of *other* navies. And because of this inexorable trend, naval cooperation with other navies is increasingly under stress. This challenge is exacerbated as nations and navies proceed along different technological development paths, as the challenges to effective networking are greater today than they were years ago when navies used simpler - and common - communications and rudimentary networking means.

The experience of the Canadian Navy in multiple deployments with US Navy carrier strike groups is but one example of the challenges that exist and persist just between two modern, technologically advanced, navies, let alone between and among multiple navies at various levels of technological maturity. Based on this documented experience - as well as other compelling data - we contend that the very technology that has helped each navy communicate among forces *within* that navy, has *impeded* effective communications with forces of other navies.

Dr.Paul Mitchell, then-Director of Academics at Canadian Forces College put this dilemma in stark terms:

> Is there a place for small navies in network-centric warfare? Will they be able to make any sort of contribution in multinational naval operations of the future? Or will they be relegated to the sidelines, undertaking the most menial of tasks, encouraged to stay out of the way – or stay at home…The 'need for speed' in network-centric operations places the whole notion of multinational operations at risk.[167]

More contemporaneously, at the 2010 Joint Warfighting Conference co-sponsored by the AFCEA and the US Naval Institute (USNI), General James Mattis, then-Commander of the US Joint Forces Command, echoed Dr Mitchell's specific themes as well as the more general themes regarding networking advanced by the CCRP when he noted:

> In this age, I don't care how tactically or operationally brilliant you are, if you cannot create harmony - even vicious harmony - on the battlefield based on trust across service lines, across coalition and national lines, and across civilian/military lines, you really need to go home, because your leadership style is obsolete.[168]

But as compelling as statements such as those above are in emphasising the importance of coalition networking, it is vital to understand the state-of-the-art today. Therefore, at this juncture, it is important to proceed to the next chapter and examine just how great the challenge of uneven technology is as a first step in examining whether there is a clear road ahead to more-effectively network the global maritime partnership.

Due to our perspective that comes from working in the military laboratory communities of Australia and the United States, our point of reference will typically begin with the five AUSCANNZUKUS nations. Based on past partnering experience, current alliance responsibilities and technological maturity of the navies involved, this appears to be the right point of departure for our discussions in subsequent chapters.

With this review of the journey of communications evolving into networking and how technological advances have enabled navies to push the edge of the information envelope and have the tactical edge over navies not as well-networked, as well as the anticipated future of C4ISR, we are ready to examine some of the challenges of networking coalition naval forces.

4. Networking Technology and Coalition Naval Force Effectiveness

Naval Coalition Networking: How Big a Challenge?

The available evidence suggests that like-minded nations committed to ensuring the rule of law on the global commons recognise the importance of coalition networking and that naval operators of all nations, the men and women 'on-point' in this effort, recognise it perhaps more so than others.

As the headquarters, acquisition and operational staffs of these navies unite in a global or regional maritime partnership to ensure their sailors can communicate seamlessly at sea, understanding the challenges to effective networking among navies - especially navies at different stages of technological development - is key to developing the optimal technical solutions. Looking to examples in the navies we represent or support - and extrapolating these examples to other navies - is an important first step in this process.

From the perspective of the RAN, *Australian Maritime Doctrine* is clear in describing the challenges of greater interoperability among naval forces, noting:

> Interoperability can never be assumed and requires substantial and sustained effort to achieve common doctrine, common procedures and common communications. The greater the commonality in equipment and methods achieved, the less duplication of resources and the fewer delays in achieving operational results when nations come together in contingencies.[169]

But how important is coalition networking and what is the 'state of play' of this networking today, especially when more technologically advanced navies and other coalition partners attempt to achieve 'shared situational awareness'?[170] Some would say that it is not yet where it should be. As Dr Mitchell noted in his article in the authoritative *Naval War College Review*, absent more effective means to network and exchange data, navies may even stop attempting to operate together. He raises what is perhaps the most important question regarding coalition naval communications - what level of communications and networking is required to make coalition operations at sea effective?

Dr Mitchell did not ask this question off-handily. For a number of years the Canadian Navy has deployed a surface combatant with US Navy Carrier Strike Groups (CSGs) for an extended six-month deployment. This is an environment where the effectiveness of coalition interoperability moves from theory to the reality of high-

tempo, forward-deployed naval operations - and operations that often involved combat. As part of his research, Dr Mitchell interviewed the commanding officers of seven Canadian ships that deployed with US Navy CSGs to determine how effectively they were able to communicate with their US Navy partners. The results indicated that while significant progress has been made, more work needs to be done.

As Dr Mitchell noted in his article, the experience of these Canadian commanding officers, as well as the experience of others working with US naval forces in NATO exercises or operations, was that the 'need for speed' in network-centric operations may result in the exclusion of even close allies. Thus, he notes, while the guiding principle of NCW is to increase the speed and efficiency of operations, coalitions are rarely concerned about combat efficiency. Rather, they are always about scarcity in terms of operational resources, political legitimacy, or both. This led him to conclude that in a dynamic coalition environment, because of the impact of slower networks or non-networked ships, the prospects of the US Navy keeping 'in step' with Commonwealth navies as well as with other likely coalition partners, is not high - absent enlightened efforts by all governments concerned.[171]

At an international C4ISR symposium Dr Mitchell put it more directly when he said during the question and answer period following his presentation:

> We have been trying to work with the US Navy for a long time. Ten years ago when we basically communicated by the red phone (tactical voice nets) we did all right because it was pretty much a level playing field. Five years ago, with Challenge Athena and the beginnings of networked communications, it started to become more difficult for us as the US Navy sped away from its partners. Today, with IT-21 and the emerging FORCEnet, the US Navy is in danger of leaving behind other navies because all of the background and decision making that goes on over networks like SIPRNET is lost to us, thus, when the order is given to do something we have none of the background for it and we are not in the battle rhythm of the operation.[172]

While some might say this is merely anecdotal information, for these authors and our colleagues from other navies - especially Commonwealth navies - the situation Dr Mitchell describes represents the reality of current coalition operations at sea and indicates there is important work yet to be done. Additionally, this is consistent with what proponents of network-centric operations have been exposing for some time. In a capstone publication of the DoD Office of Force Transformation, the late Cebrowski, considered by some to be the 'father of network-centric warfare', opined; 'The United States wants its partners to be as interoperable as possible.

Not being interoperable means you are not on the net, so you are not in a position to derive power from the information age'.[173]

If this is such an important issue then why have naval professionals not worked harder and more vigorously to solve it and why have we not found a solution yet? Part of the problem lies in the relative success that navies have had networking at sea. Even in the days of signal flags, ships at sea found a way to communicate to some degree. As technology advanced from flashing lights, to radio Morse code, to tactical radio voice circuits, to the initial tactical data links, ships at sea often kept pace with the expectations of commanders for the application of communication technology as it existed at the time. The fact that 'we've communicated at sea before and we're doing so today', often obscures how well we could communicate and exchange data if the right technology, doctrine, tactics, techniques, and procedures were in place.

For the US Navy - one of the most-likely partners of Commonwealth navies today and in the future - there is another complicating factor. Almost all officers who attain high rank in the US Navy have served as carrier strike group commanders at some time during their career, typically as their first afloat assignment as flag officers. As a CSG commander embarked in a *Nimitz*-class aircraft carrier, the communications and data exchange capabilities - with robust displays, ample switching and routing capabilities, and high bandwidth - the admiral has experienced the 'best of the best' in this area.

Additionally, from the US Navy perspective with respect to communicating and exchanging data with coalition partners, coalition nets such as CENTRIXS are likely to be installed on the aircraft carrier and that is also where coalition naval officers embark for most exercises.[174] Thus, as carrier strike group commanders mature through policy and acquisition assignments, their collective memory of coalition communications and data exchange capabilities is often quite positive - they rarely have the first-person knowledge of significant problems associated with their operational experience. But their experience is the exception, not the rule, for they have not experienced coalition networking from the position of coalition surface combatants attempting to work with US Navy ships.

High ranking Australian naval officers might have a similar lack of familiarity with the challenges of coalition networking – albeit for a different reason. One could surmise that since these officers served at sea primarily during a period when, as McCaffrie and Rahman point out in their *Naval War College Review* article, Australia had a far more minimalist approach to defence strategy and a 'continentalist' doctrine not necessarily focused on regional and global coalition operations to the extent the RAN is today.[175] Thus, without that 'corporate memory' these officers are less likely to have internalised issues regarding coalition networking than Australian naval officers serving at sea today, or even the past decade.

This is not to imply that those in charge of setting requirements or acquiring weapons systems are not keen on doing the right thing - clearly they are. However, defining operational needs, the requirements generation process, and acquisition practices have grown up over decades - even generations - and changing these processes to adequately to factor in coalition communications takes a great deal of time and attention. As yet, it is a journey that is incomplete.

Part of the reason for this lack of advocacy and difficulty in reorienting requirements and acquisition practice is the inability to quantify the 'goodness' derived from coalition networking. With naval establishments and acquisition bureaucracies increasingly driven by the rules of the marketplace - measures of effectiveness, return on investment, best business practices and efficiency - the lack of measures to quantify the benefits derived from effective coalition networking augur against spending scarce research and development, and especially acquisition, dollars to enhance something that has not yet been effectively quantified.

But it is a process that must take place if Commonwealth navies and their likely coalition partners are to operate at sea effectively for the next century. As Dr Mitchell points out in his *Naval War College Review* article, 'In network-centric warfare information is the cornerstone of all action; the existence of separate networks operating at different speeds will have an undeniable impact on battle rhythms'.[176] Clearly, overcoming uneven - or more appropriately, completely uncoordinated - C4ISR technology infusion efforts on the part of nations that would work together at sea is an essential first step in making the GMP a reality.[177] In many ways, it is a journey that has just begun.

Challenges in Networking Coalition Naval Forces

Contemporary coalition operations often require ships to operate in conditions not envisioned by their designers. The network and command and control (C2) systems of participating units reflect the operational environment they were built for, one less varied and complex than many of the missions coalition naval forces may be expected to undertake today - and tomorrow. Accordingly, effective integration of coalition naval forces challenges national policies, naval force development, and operational proficiency. Despite the history of coalition naval forces operating together and the increasing likelihood of these operations in the future, the ability of the C2 systems installed aboard warships to support coalition operations is uneven and problematic. The increasing use of coalition naval forces has revealed a wide disparity in the networking capabilities of the world's navies, an imbalance that threatens the effectiveness of the coalition naval force: it hinders interoperability and collective decision making, and prevents the force from realising its full tactical and operational potential. An assessment of the potential difficulties in building

a more effective networking capability between coalition naval forces can be considered from several perspectives.

Strategic and Political Obstacles

The strategic and political complications in networking coalition naval forces arise from the problems inherent in bringing the military forces of sovereign nations together to work towards common goals. Nations participating in the coalition operation may have limited or specific objectives for participation and these may limit or dictate the role these forces can play. Negotiating these roles as the operation proceeds will be an ongoing effort for all levels of the coalition force's chain of command and national leadership. In the meantime, the potential of the force may be lessened by the need to accommodate the restrictions placed on individual units of the force by their national leadership.

National policies can play a key role in a coalition operation by limiting and dictating the specific role national forces may play in a coalition operation. These limitations, which are not necessarily linked to operational capabilities or lack thereof, are often the result of domestic political agendas: nations join coalitions and send their forces to participate in coalition operations to meet respective national objectives. These are often a blend of global, regional, and domestic goals: gaining hegemony in a particular region, protecting economic interests, demonstrating military capability, or honouring security agreements are the most common reasons nations participate in coalition military operations.

Individual nations' objectives often limit or channel the participation of their forces, placing restrictions on the participation of forces in the coalition operation. This has a direct impact on the coalition force. For example, many countries will restrict their role to that of providing logistic support. In this case, a participating nation may send a fleet oilier or replenishment ship to participate in the coalition task force, but no surface combatants. This tailoring can be further crafted to include specific operations within the force. An example of this might be the willingness of a coalition partner to provide boarding parties for interdiction operations, but restrict their employment to engagement with vessels of certain countries.

Along with the limitations placed on forces by their respective governments comes the desire by those governments to exercise some control over their forces participating in the coalition operation. This control may be as unobtrusive and transparent to the force commander as routine logistics and administrative matters, to direct tactical orders during battle. The effects of this need to maintain a long reach back to national headquarters are most evident in two ways. First, consultation and waiting for direction from national leadership will slow the participants' performance in force operations. Second, the need to maintain communication with national leadership places a burden on the communications

resources aboard each unit, impacting that unit's ability to network with other members of the coalition force.

Operational and Tactical Obstacles

Building a coalition naval force is challenging not only in the planning and high level decision making associated with assigning forces but in the routine management of the forces assigned to the coalition. The operational capabilities of units assigned to a given coalition operation may be uneven and difficult to integrate. This might be because the capabilities of some of the units may not match those of the rest of the force, but their inclusion is deemed necessary from a diplomatic or political perspective. This is most evident in the area of tactical capabilities where some of the units might not possess the speed, endurance, or reliability of the rest of the force. Older units assigned by smaller navies from poorer nations may not add much in overall capability to the coalition force. Additionally, the crews of some units assigned to coalition forces may not have the same skill level as the rest of the force, adding to the imbalance in capabilities or gap in force capability.[178]

In practice, coalition naval forces must deal with the disparity in force capabilities through the on-scene operational efforts by the commanders and commanding officers of the force. Astute assignment of duties among the force will allow the smallest and least capable of units assigned to roles where their limited capabilities may still make a contribution to the force. Allowing additional training for less experienced units of the force, particularly if mentored by more skilled navies, can even add to the benefit of the operation by bolstering allied naval potential and cementing navy-to-navy professional ties. Because of this, mutual training and exercising basic seamanship, aviation, and tactical skills often becomes part of the coalition's mission.

Programmatic and Economic Obstacles

Programmatic and economic difficulties in networking coalition forces arise from the different approaches coalition navies take in procuring their networking capability. While the US Navy and other larger navies may follow a long-range plan for improving networking capability over time, smaller navies do not always budget for long-term improvement and keep originally installed capabilities longer.[179] The procurement policies of most small potential coalition partner navies are geared towards a limited afloat capability in networking that is focused on smaller ships with a fixed set of missions. This may drive the capability on these ships to a more modest networking capability - such as limited IP bandwidth - than is found aboard, for example, US Navy ships. Additionally, the procurement policies in most potential coalition partnering navies will be primarily focused on the purchase of indigenous networking capabilities, linked to national command

and control systems. This may make it difficult to match these capabilities up with US Navy and other navies' networking capabilities.[180]

The networking capability of potential coalition partner navies will depend on the choices individual navies make in regards to the types of networking systems they build into their forces. The specific mix of these systems brought by a particular navy is usually based on the need to employ ships in regional waters in scenarios that reflect these regional priorities. Moreover, these choices in networking capability usually reflect the employment of naval forces in traditional warfare roles, based on a ship's primary mission such as ASW, AAW or mine countermeasures. However, today's coalition forces are often engaged in new and non–traditional missions: anti-piracy, maritime interception operations (MIO), disaster relief, and others.

Determining Coalition Naval Networking Force Requirements

Modern networking capabilities offer the prospect of enhanced interaction between decision makers and planners in managing coalition naval forces. As businesses and individuals in their personal lives have discovered, these networking capabilities can help overcome the natural barriers to communication between people and to collaboration and working together.[181] Issues that are related to language, culture, and command structure, so difficult to breach with older and less flexible communications systems, are more easily dealt with by contemporary networking tools and applications such as text chat, email, and video teleconferencing. This translates to quick, decisive action within a coalition force.

Command and control of coalition naval forces must provide for several interrelated but discrete efforts. These efforts, directly related to tactical and operational tasks and requirements, require networking at several levels to ensure that the coalition force can operate safely and effectively. The appendix (at the end of the publication) attempts to simplify this potentially complex problem by matching basic C2 activities undertaken by coalition naval forces to the networking 'systems' available to these forces.[182]

Tactical Coordination

The most straightforward C2 need for a coalition naval force is that required at the tactical level, essentially that required for the safe navigation and manoeuvring of the force. The tactical coordination within the force must also allow for the integrated safe and effective employment of weapons systems.

The needs of tactical coordination among the coalition force from a networking perspective are straightforward. Passing of tactical orders must be done quickly

and with clarity. During coalition operations two factors are particularly important, the use of a common language and agreement as to basic tactical rules. The former is usually addressed by the use of English. English is mandated as the standard language for naval tactical information by several treaties and English has the added benefit of being the most commonly used language for seafarers and aviators by international convention.

The use of common operating procedures and tactics amongst coalition forces can be more difficult. Again, treaties, multi and bilateral agreements may be used as an underpinning for common procedures in tactical formations, manoeuvring, and the assignment of responsibilities. However, these must usually be supplemented by amplifying directions and special procedures directly related to the nature of the force's mission. These amplifications, in the form of operations orders (OPORD), operational taskings (OPTASK), fragmentation operations orders (FRAGO), and intentions, must be published in advance, usually after consultation amongst the senior officers of the force.

Force Level Planning and Coordination

Recent coalition naval operations as varied as counter-piracy patrols in the Indian Ocean and humanitarian relief off Haiti point to an obvious fact: coalition naval task force missions can be complex and cover a wide range of operations. Planning for these operations is usually undertaken at short notice, and over the large distances that can separate national capitals, deployed naval forces, and remote operating areas. Undertaking the planning needed to effectively build and employ a coalition naval force requires the support of a networking capability that is dispersed, increasingly robust, and capable of providing commanders access to a wide range of data and instantaneous communications.

Planning for coalition operations can be thought of as occurring on two levels. At what might be considered the senior level, commanders and national leaders need to interact to ensure that respective national goals are addressed in the mission assigned to the force. On a lower level, action officers, unit commanders, and supporting forces work out the specific roles for each of the elements of the force. Each of these levels presents unique challenges to the networking capabilities of participating nations. At the senior level, political and high-ranking military leadership from the countries involved must articulate national policies and objectives, negotiate assignment of forces and their roles, and address the usually delicate issue of authority and 'chain of command' for the force. At the lower level, the specific and detailed issues of task force responsibilities, logistic support, operating restrictions and limitations, and rules of engagement must be discussed, resolved and finally instantiated into instructions for the units of the force.

The general division of labour in planning for coalition force operations provides an insight into the type of networking capability required to support both levels. Planning for coalition operations is marked by extensive personal interaction between leadership and detailed collaboration between action officers and specialists. Senior leaders, in particular, enjoy 'face-to-face' communications while planning, and this direct interaction has in practice extended down to the senior military leadership. In the case of senior afloat commanders in a naval coalition task force, this can be difficult in view of communications capability limitations. Action officers, faced with the responsibility of working out myriad details quickly, need to be able to quickly exchange documents and converse with each other. In addition to informal exchanges in support of the planning process, the final establishment of a plan for the coalition force will require a formal briefing for commanders and principals. This briefing will also be challenged by distance, communications capability, and time.

National Command and Control

Coalition naval force deployment generally occurs in response to an international crisis or event with significant impact for the nations involved. In committing naval forces to the situation, the nations in question are signalling a strategic interest in the situation and a commitment to a resolution of the situation in a manner consistent with their own national goals. Moreover, the commitment of naval or military forces represents a risk: poor performance by the forces will not only be an embarrassment, but could threaten the readiness of the nation's military forces and potentially encourage action by the nation's enemies. Accordingly, nations participating in coalition naval force operations retain some measure of control over their forces even while they are deployed with the coalition force.

Coalition forces will certainly bring their native networking and communications suites with them when they join the coalition force. However, the adequacy of these systems to address the unique requirements of coalition operations is often problematic. Smaller navies build communications and networking capabilities that are essentially regional and may be ill-suited to communicating with respective national command structures over greater distances. In addition to taxing the equipment needed to establish communications with its home headquarters, the technical personnel assigned to a coalition force unit will be busy in supporting intra-task force communications, potentially hindering both networking with the headquarters and the rest of the coalition force.

Networking Capabilities for Coalition Naval Forces

The above requirements for networking coalition naval forces require a range of technological capabilities. These networking capabilities, as design choices for naval units, can be divided into four categories by their impact on the potential of the units to participate in coalition force operations: voice communications, written record communications, tactical data systems, and IP-based services. There is a natural hierarchy among these capabilities and the specific systems that provide them. However, they are synergistic and complementary. Some of the technology providing a specific set of capabilities may also supplant the need for individual systems, realising design efficiency in terms of reduced crewing, smaller footprint, and enhanced performance.

The Appendix summarises the application of the four general categories of networking capabilities with the three general requirements for C2 within a coalition force. In doing so, the relative advantages of one capability over another are made evident in relation to the specific task being undertaken. These matchings are not absolute, but are representative. They serve to highlight the advantages of different types of networking capability and, accordingly, the impact of these capabilities on coalition naval operations.

Voice Communication

The simplest form of networking and the most common within a coalition naval force, voice communication between ships remains a staple of the networking capabilities required for these forces. Done with a variety of radios employing a range of waveforms across the electromagnetic spectrum, contemporary naval forces can rely on voice communication over varying distances, with generally predictable reliability.

For the most part, naval forces rely on HF, VHF, UHF for ship-to-ship communications. These systems work without the need for satellite support, from line of sight (UHF) to hundreds of miles (HF). In addition to the ship-to-ship mode for radio voice communication, UHF and super high frequency (SHF) shipboard installations can take advantage of satellites for increased range. This capability is restricted to newer ships in some navies and may not be available throughout the coalition force. Similarly, the relatively recent use of Voice Over Internet Protocol (VOIP) has expanded the potential for ship-to-ship voice communication to the use of desk telephones between ships.

Despite its ubiquity and central role in coalition naval operations, voice communication has several drawbacks. Viewed from a data rate and data content perspective, voice communication is limited: the ability to pass data is bounded by

the human cognitive processes of speaking, listening, and recording. From a data perspective, information sent over voice must be processed and disseminated at the receiving terminal, with the high probability that misunderstanding, misinterpretation, or missing data will obscure the content. Additionally, voice communication is a relatively slow means of passing data, a limitation that is obvious in a fast-paced tactical situation. Finally, language and the cognitive process associated with it can lead to ambiguity and confusion when relying on voice communication.[183]

These limitations aside, voice communication is an important means of networking the coalition naval force for several reasons. The ability of decision makers and action officers to speak directly to each other can eliminate layers of the chain of command and confusion. The 'give and take' of verbal communication can be particularly important in the often delicate business of coalition coordination. Finally, verbal communication via radio allows limited but essential human interaction, with its subtlety and nuance. This can form the basis of interpersonal relationships that are critical in coalition operations.

Written Record Communications

The use of written record communications has been a fundamental means of networking since the beginning of the twentieth century. Having evolved from the use of Morse code and transcription by hand to today's high-speed teletype systems, record 'traffic' is the formal means for passing orders between headquarters, ships, and their embarked commanders. It is secure, sent over nationally owned radio links, encrypted and easy to limit in its distribution. Accordingly, its processing and dissemination are still manual, labour intensive, and time consuming, although automation over the past several years has broadened the distribution of message traffic to commands supported by local area networks (LAN) and Internet-like services.

Because of agreements and conventions among the AUSCANNZUKUS navies, message traffic can be sent from ship-to-ship and unit-to-unit. This greatly simplifies the process of sending formal coordination information and orders among coalition forces made up of the 'five eyes' nations. However, as a data type, the official 'message traffic' is difficult to process. Because message traffic sends only words in a standard 64 character set format, complex instructions must be spelled out and cannot be supplemented with graphics or diagrams. Message traffic must be read and interpreted by a human being and complex instructions may be subject to misinterpretation. Most importantly, the channels for passing message traffic operate slowly over the radio spectrum. Even satellite based message traffic moves slowly through the system between originating command, communications station, to terminus; and during high tempo operations, which coalition operations tend to

be, the backlog of message traffic can become pronounced. The lack of timeliness in these situations can contribute to misunderstanding and operational error.

Tactical Data Systems

The tactical data systems employed by forces afloat pass specific operational data in a graphic format, usually a geospatial display that supports rapid evaluation of the tactical situation for decision makers. Tactical data systems are usually tailored to the operational environment - ASW, AAW, and so forth.

A variety of tactical data systems are currently used by coalition forces. The United States-developed Link 11, 16, and 22 systems are a standard employed by most first line ships and aircraft of the AUSCANNZUKUS navies. The combat systems of these units, for example the US Aegis system or the UK Principal Anti-Air Missile System (PAAMS), is the primary source of information for the Link, allowing the tactical 'picture' available in each unit to be shared with other force units equipped with the Link system. The Link system also allows the automated passing of force orders: the force commander can order a unit to engage - or 'take' - a target via Link. In support of this, tactical data systems have a basic decision support capability built into them. These capabilities include prioritisation of threats, recommended engagement assignments, and intercept and avoidance recommendations.[184]

Tactical data systems such as Link have been in service for over 40 years and have evolved, with newer systems offering networking capabilities beyond the basic functionality described above. The US Global Command and Control System (GCCS) provides more extensive data on land based, air, and maritime units, although its locating data is less precise than Link. The Cooperative Engagement Capability (CEC) provides for the compilation of accurate targeting data from radar measurement data distributed between ships and aircraft. These system and other complimentary systems with an expanded scope of information are commonly referred to as the Common Operational Picture (COP) and allow the sharing of tactical relevant data beyond the force and with higher headquarters.[185] However, sharing COP data across national lines can be cumbersome. For example, the US and other NATO navies have developed protocols and applications to share the COP, but other navies with less developed communications systems and networks have not been able to receive this more comprehensive data.

As a networked system, tactical data systems suffer from the disadvantage of being closed or 'stovepiped' systems with dissemination restricted to units with dedicated installations. In coalition forces, the individual tactical data system installation varies with the type of units assigned. Older and smaller units may not have the same tactical data systems as the larger primary units, impacting their ability to be integrated into the force's tactical planning.

IP-Based Services

The use of Internet Protocol (IP) network services has become increasingly common in the planning of military operations. The flexibility of IP allows it to support a range of services, allowing users access to a range of tools that have become common in daily life and are similarly useful to military forces. Tools and applications such as email, websites, shared applications, video over IP, and even social networking tools are available over IP networks and have demonstrated a highly useful role in naval force operations.

The tools and services available over IP networks are particularly suited to complex operating environments for today's coalition naval forces, where the mission may be outside usual tactical environment and require comprehensive interaction between decision makers. MIO, humanitarian assistance (HA), disaster relief, and counter-piracy all require extensive interaction among planners, commanders, political leadership back at home stations and headquarters. The information required for these types of operations is more complex than that stored by the tactical data systems outlined above and may require various types of documents, graphics, photographs, numeric data, etc. to allow planners to adequately plan operations. Text chat, email, VOIP, and video particularly are valuable for the collaboration necessary to execute sophisticated operations that are beyond the standard preplanned tactical actions in established coalition naval doctrine.

Although valuable and increasingly common in military planning, IP network services are difficult to provide to forces at sea. The primary reason for this is the difficulty of providing broadband IP service to ships. Relying on radio frequency (RF) signals for providing connectivity, ships at sea are faced with a shortage of radio assets to meet the demands outlined above, including voice communications and tactical data systems. Providing broadband IP connectivity with these same limited radios resources compromises capabilities and even capital ships have a relatively modest IP bandwidth capability in contrast with major shore C2 nodes. Smaller coalition combatant ships typically have a much more limited radio capability and correspondingly more limited access to bandwidth for IP services.[186]

Results of Uneven Networking Capability within the Coalition Naval Force: The Plane Guard Syndrome

The disparity in C2 and networking capabilities among a coalition naval force ultimately can impact the operational capability of the force. Coalition force commanders faced with the task of organising the coalition task force on the spot tend to assign units with lesser C2 and networking capabilities limited roles where robust C2 and networking are not required. For example, coalition surface combatants without robust networking capabilities - tactical data link systems (TADIL), IP - are sometimes assigned plane guard duties, which have the minimal C2 requirements of simple voice and visual signalling, when these units are attached to US carrier strike groups. While a plane guard assignment fills a vital safety role, the relegation of coalition ships to such duties often fails to leverage their full tactical potential. Assigning coalition naval units to plane guard and other lower priority tactical roles can also risk offending national sensibilities, leaving the coalition unit assigned such lower priority duties the impression that their contribution to the force is under-appreciated and underutilised.

Naval C2 planners have applied the term 'heterogeneous' to naval forces with mixed network capabilities.[187] Underlying this aggregate characterisation are the individual capabilities of each ship in the force and the impact the lack of networking capabilities has on both the individual ship and the force overall. Ships lacking in modern networking capabilities find themselves restricted in the role they can play in coalition naval operations. These roles are often less than might be expected from the individual ship's design capabilities and ships with limited networking capacity often find themselves performing conventional and simpler tasks.

The impact of this underutilisation occurs at several levels. First, the coalition naval force can be deprived of the full capability of the under-equipped ship. Its sensors are less effective without the cueing networking provides. Its weapon employment is similarly hampered by the inability of its combat direction system to gather targeting data available on the network.[188] Finally, the command structure of the poorly networked ship - commanding officer, operations officer, tactical action officer or principal warfare officers (PWO) - is isolated from that of the force, preventing it from collaborating with the force commander and participating in the joint planning so necessary for coalition operations. Moreover, integrating ships with lesser networking capability can take disproportionate effort on part of the force's command structure.

The tactical effect of the isolation associated with less-than-robust networking capability is immediate and is realised in decreased operational effectiveness of

the force. Longer term, but just as potentially debilitating, are the effects that a decreased networking capability may have beyond that of the current operations. The crews of ships with relatively poor networking capability do not have the opportunity to train in the modern tactical and operational roles they may need to for the future. This is particularly important because these coalition operations are often undertaken in regional waters and the coalition operation can be a first step towards long-term political stability. The crews of these ships are often well versed in the operating environment and their greater participation in key networked tasks would be of benefit to the coalition force's leadership. However, the inability to use modern networking technology can relegate these ships and by extension, their navies, to second-tier roles in the coalition force's mission. This, in turn, can even result in perceived insults, tensions among the force, and potential damage to relationships between nations engaged in the operation.

Additionally, many of the missions undertaken by coalition forces benefit from the participation of regional naval forces, which may be lacking in networking capability, but are rich in local information and understanding of issues that might impact the success of the force. Contemporary coalition naval missions may be providing humanitarian assistance, disaster relief, restoration of civil affairs, and maritime interdiction, all of which require detailed understanding of local tactical and political conditions. The ability of regional naval commanders to provide timely and relevant advice to the coalition force commander in these areas can be hampered by poor networking capabilities.

Addressing the Gap: Working towards Common Networking Capabilities

Implicit in the above discussion of uneven and heterogeneous networking capabilities is the need to enhance the networking capability of coalition naval forces. Clearly, all potential coalition partners will not be able to develop an at-sea networking capability similar to the Commonwealth navies or the US Navy. A framework is needed that will allow the operational logic of the Appendix to be translated into procurement plans that can give coalition partners selected capabilities based on their resources and anticipated operational requirements. Two elements are critical to such a framework. The first is a well-thought-out mapping of the capabilities called for in the Appendix to networking technologies. This mapping needs to support the establishment of technical requirements linked to network capabilities. Two immediate tools are available. First is the NATO Network Enabled Capability (NNEC) C2 Maturity Model. This model allows C2 planners and engineers to develop the proper metrics and assessment tools for evaluating network capability in a given situation with a given force.[189] A second tool that can be used in guiding technology development for networking

coalition naval forces is the US Navy's FORCEnet Functional Capabilities. While the term 'FORCEnet' is being supplanted by new terminology, nonetheless the fifteen required functional capabilities for FORCEnet, together with their specified metrics, still provide a useful taxonomy for the development of specific technical capabilities for networking naval forces.[190]

A second requirement for moving forward with enhanced coalition networking capability is a collaborative effort among potential coalition partners that will facilitate the technology development addressed in the previous paragraph. This needs to be a formal nation-to-nation effort among naval officers, national defence policy makers, scientists, and engineers. A description of how this currently works within the Commonwealth and the United States is described in the following chapter and is offered as a possible model for other efforts. In the meantime, immediate solutions can include the temporary loan of networking and communications equipment to coalition units, as has been done with the CENTRIXS system loaned by the US to nations such as Singapore and other nations for specific operations.[191] This stopgap approach may be necessary during crises to facilitate immediate operations, and it helps raise the awareness of current networking capabilities within smaller navies.

5. Nations and Navies Working Together More Effectively

How Can this be Achieved?

As we have pointed out in Chapter Four, the challenges to effective coalition networking are indeed daunting. And given the long history of nations and navies attempting to collaborate at sea in a coalition environment, it is quite easy to reach the conclusion that if the solution were simple, it would have evolved already. But rather than an impediment, the fact that a solution still eludes us should be reason enough to accelerate efforts to address this important need. For Australia, given its extensive engagement with other navies regionally and even globally, the need for the ADF and the RAN to seamlessly interoperate with partners is especially acute.[192]

That said, finding a solution to effectively networking *all* potential coalition partners in the near term is a challenge that may be a literal, 'bridge too far'. However, what this chapter will demonstrate is that starting with a nucleus of navies that operate at or near the 'high end' of naval capabilities could be an important first step - a 'beta test' to provide a way ahead for a longer-term effort to ensure that navies seeking to secure the global commons are able to interoperate with each other. And based on our work with the AUSCANNZUKUS nations we represent, we believe this effort must begin at the laboratory level in each of our defence establishments.

Out of the Labs: Achieving Coalition Networking

Few would argue that the challenges to achieving effective networking at sea and to devising and co-evolving C4ISR systems for navies, even navies with such similar traditions, platforms and technologies as the five AUSCANNZUKUS nations, are simple to solve or demand anything less than a full-on effort on the part of government defence laboratories to work together to address these challenges.

However, the scientists and engineers working in these government defence laboratories also recognise that the ways and means for them to work with their colleagues in other nations must be well-developed and robust enough to ensure a coordinated effort. A primary means for accomplishing this work is through bilateral agreements between two nations in the form of Data Exchange Agreements (DEA) or Information Exchange Agreements (IEA).

From the principal researcher level and up through the leadership levels of these laboratories, scientists and engineers are keen to use these bilateral DEA or IEA to facilitate their work with their fellow scientists and engineers in laboratories in the other AUSCANNZUKUS nations. But the task of devising a DEA or IEA and then getting it approved through a substantial review chain in the respective nations involved is not trivial. We have first-person experience working with DEA and IEA in our respective laboratories. Forging these agreements is a time-consuming process and the time-lag between articulating the need for a DEA or IEA and having it approved and 'in place' is often substantial. Moreover, once complete, these agreements are most-often between just two nations.

Fortunately for AUSCANNZUKUS nations, recognising the shared interests these five nations have, as well as the somewhat-limiting nature of bilateral defence exchange agreements, the respective governments have put in place a network of agreements that enable the exchange of scientific and engineering information at the defence laboratory level. This network of agreements is captured in a publication called *A Beginner's Guide to the Technical Cooperation Program*, which provides an explanation of the purpose and construct of each of these organisations that oversee information exchanges in more detail.[193] A listing of these groups is provided below:

- ASIC: Air and Space Interoperability Council (Australia, Canada, New Zealand, United Kingdom, United States) - focused on aerospace interoperability.
- ABCA: American, British, Canadian, and Australian armies (Australia, Canada, United Kingdom, United States) - focused on army interoperability.
- AUSCANNZUKUS (Australia, Canada, New Zealand, United Kingdom, United States) - focused on naval command, control, communications, and computers.
- CCEB: Combined Communications Electronics Board (Australia, Canada, New Zealand, United Kingdom, and United States) - focused on military command, control and communications.
- MIC: Multinational Interoperability Council (Australia, Canada, New Zealand, United Kingdom, United States) - focused on military interoperability.
- MIP: Multilateral Interoperability Program (Australia, Canada, United Kingdom, United States) - focused on command, control, and interoperability.

- TTCP: The Technical Cooperation Program (Australia, Canada, New Zealand, United Kingdom, United States) - focused on military science and technology.

Our personal and professional experience - while intersecting and mapping to several of the organisations above - is primarily focused on our years-long work on a Technical Cooperation Program team. Understanding how this team evolved and focused its work in developing a way ahead for effective coalition networking at sea is necessarily preceded by an understanding of TTCP writ large.

The Technical Cooperation Program

Although it has been around in various forms for almost half a century, TTCP is not universally well known, even by Commonwealth naval personnel, and some background is in order to explain how this program facilitates efforts to address coalition interoperability. Importantly, while conducting an analysis of coalition interoperability in another forum is certainly *possible*, the extant TTCP organisation and infrastructure provided a ready-made medium that made success in this endeavour *probable*.

TTCP is a forum for defence science and technology collaboration between Australia, Canada, New Zealand, the United Kingdom, and the United States. It is one of the largest collaborative defence science and technology activities in the world. The statistics alone give some indication of the scope of this effort: five nations involved, 11 technology and systems groups formed, 80 technical panels and action groups up and running, 170 organisations involved, and 1200 scientists and engineers directly accessed. By any measure, TTCP is a broad-based effort that tremendously facilitates science and technology cooperation among the five member nations.

TTCP can trace its origins back to 25 October 1957, when the President of the United States and the Prime Minister of Great Britain made a Declaration of Common Purpose containing the following:

> The arrangements which the nations of the free world have made for collective defence and mutual help are based on the recognition that the concept of national self-sufficiency is now out of date. The countries of the free world are inter-dependent and only in genuine partnership, by combining their resources and sharing tasks in many fields, can progress and safety be found. For our part we have agreed that our two countries will henceforth act in accordance with this principle.[194]

Immediately afterward, the Canadian government subscribed to this principle of interdependence and joined in the common effort. The resulting organisation was

called the Tripartite Technical Cooperation Program (TTCP). As a result, the World War II-era Combined Policy Committee was reconstituted and the Subcommittee on Non-Atomic Military Research and Development (NAMRAD) was established. It comprised of the heads of defence research and development organisations in Canada, the United Kingdom, and the United States. Australia joined the NAMRAD Subcommittee in 1965, and New Zealand joined in 1969, at which point the organisation governed by the Subcommittee was renamed The Technical Cooperation Program (TTCP).

The development of TTCP came at a time of increasing collaboration between and among the allies of the newly-formed NATO. In 1957 and after three years of deliberations, the CANUKUS (Canada, United Kingdom, and United States) ratified the technical standard for data exchanges, one of the first efforts to set common standard for information technology used in the naval context. Originally named the Tactical International Data Exchange (or TIDE, 'good for cleaning up messy tactical pictures') it later became known as Link 2 (given as II in roman numerals in the Royal Navy, which was already using forms of data-sharing technology to distribute tactical information among its ships). As other NATO links became established, Link II became known as 'Link 11'.[195]

As systems became more technically complex and the need for cooperation between the new NATO allies grew, organisations such as TTCP became more vital as a ready-made means to collaborate at the basic science and technology level. The aim of TTCP is to foster cooperation within the science and technology areas needed for conventional (non-atomic) national defence. The purpose is to enhance national defence and reduce costs. To do this, TTCP provides a formal framework that scientists and technologists can use to share information among one another in a quick and easy fashion. And as noted in the 2009 Defence White Paper, TTCP is the *prime* multilateral science and technology relationship used by the Australian Defence Organisation and specifically the Defence Science and Technology Organisation to enable its support for joint organisations including Capability Development, Joint Operations and Defence Materiel.[196]

Collaboration within TTCP provides a means of acquainting the participating nations with each other's defence research and development programs so that each national program may be adjusted and planned in cognisance of the efforts of the other nations. This process avoids unnecessary duplication among the national programs, promotes concerted action and joint research to identify and close important gaps in the collective technology base, and provides nations with the best technical information available.

TTCP has its centre of gravity in the applied research domain, but it also encompasses basic research and technology development activities. The scope includes the exploration of alternative concepts prior to development of

specific weapon systems, collaborative research, sharing of data, equipment, material and facilities, joint trials and exercises, and advanced technology demonstrations. Cooperation within TTCP often acts as the catalyst for project-specific collaborations further down the equipment acquisition path.

TTCP consists of three levels and thus has a streamlined hierarchy that promotes five-nation cooperation. Level 1 is the strategic policy level and comprises three groups of personnel: the Principals, the Deputies, and the Secretariat. Each nation has one representative to each of these groups, with the exception that the Australian Deputy also acts as the New Zealand Deputy. The Principals make up the NAMRAD Subcommittee. The Deputies and Secretariat are all based in Washington, DC, and collectively form the Washington Staff.

Level 2 is the program planning and oversight level and currently contains 11 Groups, each focused on a particular technology or systems area. The Groups have an Executive Chair (appointed from any one of the nations), up to five National Representatives, and a number of Technical Advisors. Finally, each Group has one Deputy assigned to act as its Group Counsellor (GC), who works with the Group to help communicate the Principals' strategic direction. The Groups are: Aerospace Systems; Command, Control, Communications and Information Systems; Chemical, Biological and Radiological Defence; Electronic Warfare Systems; Human Resources and Performance; Joint Systems and Analysis; Land Systems; Maritime Systems; Materials and Process Technologies; Sensors; and Conventional Weapons Technology.

Level 3 contains bodies that sit under each Group and actually perform the collaborative activities. There are three types: the semi-permanent Technical Panels (TP); the temporary Action Groups (AG); and the project-specific Project Arrangements (PA). Technical Panels are designed to manage a continuing program of work and will generally oversee a number of subordinate activities. Action Groups are initiated to investigate a specific issue and, on completion, will recommend if and how any further work on the subject should be undertaken on a more permanent basis. Project Arrangements are a more binding form of cooperation, used to support a specific project or collaboration.

Technical Panels and Action Groups have a Chair, plus National Leaders for each participating nation and a varying number of Team Members. Not all nations participate in all TP or AG. The majority of personnel involved in TTCP operate at or in support of Level 3. The structure at Level 3 can and should evolve to remain relevant. Groups have the authority to initiate and terminate TP and AG, although the changes must be notified to the Principals at their next annual meeting.

TTCP operates by sharing the output from existing national science and technology programs for the greater benefit of the participating nations. It is therefore

fundamentally a bottom-up organisation, with collaborations occurring only where national programs and a willingness to cooperate already exist. The role of the Principals and National Representatives in managing TTCP therefore takes two forms: directing collaborations within areas where suitable national programs already exist; and directing their own national programs in order to provide the basis for future TTCP collaborations. TTCP is thus a 'best endeavours' organisation and can only be as good as the underpinning national programs.[197]

Today, TTCP operates under an updated Declaration of Common Purpose that informs the efforts of the organisation's Technical Panels and Action Groups. This declaration states:

> No member nation possesses the total resources to provide for its own defence research and development (R&D) needs. Each must assist the others by sharing resources and tasks in many fields so that all can find progress and security. The aim of TTCP then is to foster such cooperation in the science and technology (S&T) needed for conventional national defence. The purpose is to enhance national defence at reduced cost.[198]

With this description of TTCP as background, we are ready to understand the work that has been conducted under the auspices of the Maritime Systems Group (MAR) Action Group 1 (AG-1) Net-Centric Maritime Warfare Study and Action Group 6 (AG-6) FORCEnet Implications for Coalitions. This section of the book reports on the past six-plus years of activities and the way ahead for the ongoing research of this group.

One Example of Commonwealth Labs - Plus the United States - Finding Networking Solutions

Action Group 1 (AG-1) Net-Centric Maritime Warfare Study

Much has been written, primarily from a qualitative perspective, about the perceived benefits to the military of transforming from a platform to a network-centric force structure.[199] However, few such studies have taken an analytic view and produced quantitative results, and fewer still have done so in the context of broadly based coalition operations.[200] In response to a mutually perceived need, the five allied countries of TTCP Maritime Systems Group established Action Group One (AG-1) in 2001 to conduct a three-year (October 2001 to September 2004) 'Network-Centric Maritime Warfare (NCMW)' collaborative study. The objectives of this study were to provide TTCP MAR Group, as well as national

military customers, with guidance on, and analysis of, the implications of NCMW for coalition maritime force capabilities, C4I interoperability, and to help shape national acquisition strategies.

The Terms of Reference (TOR) for AG-1 charged the group to examine and help establish the first principles of 'force-netting' from a coalition and distributed systems perspective, and to research the analysis methods needed to quantify the benefits of networking in coalition operations. Armed with the TOR, as part of its study definition AG-1 members consulted with national and international military staffs to determine a priority list of issues to address. Ultimately, the group decided to analyse and quantify the military utility of selected parametric levels of network-centric capabilities by addressing tactical information exchange, in rigorous analytical detail, for three selected tactical situations (TACSIT) associated with coalition maritime littoral warfare: Maritime Interception Operations (MIO), Anti-Submarine Warfare (ASW), and Anti-Surface Warfare/Swarm Attack (ASuW-Swarm).

AG-1 first met in October 2001 to review and understand the TOR and to map out methodology to address the MAR guidance. The group decided that to address the issue of NCMW properly, two studies were needed: Study A, a broadly-based higher level study addressing overarching NCMW analytical issues and 'first principles' of force networking from a coalition and distributed systems perspective; and Study B, an in-depth focus on the three tactical situations noted above that, together, represented a spectrum of different types of coalition-force maritime tactical situations of high interest to TTCP nations.

Understanding the *process* of selecting these studies provides insight into the dynamics of international cooperation in science and technology under the auspices of TTCP. Study A, the broad area study, selected operational planning and intelligence, surveillance, and reconnaissance (ISR) as the area of focus because all five coalition partners participated in it to one extent or another. For Study B, the range of tactical situations to select from was quite extensive. One of the first orders of business for AG-1 was to conduct a survey of coalition contingency operations that occurred most frequently among the member nations. Once this list was compiled and the list of possible tactical situations to examine was narrowed down, the candidate list was vetted with uniformed AUSCANNZUKUS professionals from the five member nations. Ultimately, three missions, MIO, ASW, and ASuW (specifically against the swarming small boat threat), were selected for study. Additionally, and serendipitously, for each of these missions, the partnership among the five nations was on a more-or-less equal footing.

While a full report on AG-1 efforts and results is subject to restrictions on its release and precludes directly citing many TTCP MAR AG-1 documents, understanding the *process* that AG-1 used to obtain their results gives a clear window on this

effort and helps to understand the best practices this group used to inform future efforts of this nature.[201] Significantly, in addition to investing substantial effort to select focus areas where all coalition partners were on an essentially equal footing, the study participants conducted 'due diligence' to review and understand the various analysis methodologies available to conduct AG-1's work. In fact, one of the AG-1's early reports provided an extensive review of analytic techniques appropriate for the group's work, and the contents of this report informed each of the studies undertaken by MAR AG-1.[202]

Armed with an agreement regarding the studies to be conducted and with several analytic techniques potentially appropriate to both Study A and Study B, MAR AG-1 set about addressing the MAR direction expressed in the TOR and conducted the two major studies in parallel. Within Study B, MIO, ASW, and ASuW were addressed in that order. Significantly, no one nation provided all of the analytical techniques applied. Rather, for each study the group drew upon the analytical expertise of each member from a 'nation-blind' perspective and ultimately selected the analytical technique most appropriate to the tactical situation at hand. Serendipitously, the operational requirement of the various tactical situations drove the team to select a mix of analytical techniques for the studies, ensuring that the work of the team was not narrowly focused on the preferred analytical methodology of any one nation.

The results of Study A were significant and important to the overall conduct of Network Centric Maritime Warfare and stemmed from the hypothesis that NCW is the core concept for enabling a new revolution in military affairs for the information age. This concept postulated that greatly increased combat power derives from the ability of a highly connected system of entities, widely distributed throughout the battlespace dimensions of space, time, force, information, and cognition, to rapidly concentrate influences to deliver decisive effects on an enemy while minimising the exposure of friendly entities.

Importantly from the standpoint of addressing the issue of networking the global maritime partnership, Study A was also based on the proposition that the complexity of the networked force will demand a co-evolution of systems, technology, and doctrine. It also notes that while force experimentation has been adopted as a co-evolution mechanism, it is not feasible to explore the requisite paths by experimentation because attempts to do so yield heuristics that create a risk of misunderstanding the gap between experiment-observed and battlespace-realised capability. Thus, Study A showed that appropriate analytical methods need to be applied to adequately explore the problem space in a timely, tractable, and affordable manner. Further, it showed that these may be based on systems-engineering techniques, but the conceptual description of distributed networked systems and their behaviour requires further development before systems-engineering principles can be applied.

Thus, Study A mapped the broad parameters and issues that are addressed in quantitative modelling of NCW. It also showed that conceptualising NCW requires paying much more attention than heretofore to the information and cognitive domains of warfighting - domains that have always been important - but have not had much analytical attention to date. Study A further noted that models of NCW must include representations of information, the manner in which it arises from data generated in the physical domain and its flow around the information domain.[203]

With Study A providing the broad underpinnings of the work of AG-1 the team undertook detailed analysis of the three aforementioned tactical situations (MIO, ASW and ASUW/Swarm). These TACSIT were each carefully designed to strike a balance to enable them to be generic enough to be of general relevance but also specific enough to support and inform each nation's requirements-generation process and acquisition programs. This careful sculpting and dimensioning of each TACSIT was a key factor that enhanced Study B's utility to each nation in particular and to the analytical community in general. A brief description of these TACSIT and their development is presented below, and more robust treatment of each TACSIT is cited. These studies are part of the body of work maintained by the Command and Control Research Program.[204]

A. Maritime Interception Operations (MIO) TACSIT

The first tactical situation examined by MAR AG-1 was MIO. This represented a tactical scenario familiar to all the member nations, and one that all believed they would be involved with in the future. Additionally, the member nations recognised that the results of this study would be important to each nation since the operational experience of all navies was increasingly focused on a particular aspect of MIO. Thus, MIO provided an excellent first study for the participants. The results of this study reported in this book are extracted primarily from the report of the MIO TACSIT Group, presented at the 8th International Command and Control Research and Technology Symposium.[205]

From AG-1's initial investigations a number of hypotheses about tactical NCMW applications were developed to address a variety of tactical level war-fighting scenarios. The hypothesis for MIO was:

> *In coalition force MIOs, network-enabled collaborative planning/ re-planning increases the probability of intercepting a contraband vessel.*

The associated null hypothesis is that network-enabled collaborative planning/ re-planning does not increase the probability of intercepting contraband vessels.

MIO can form a large part of both peacetime and wartime naval operations, particularly for mid-size and smaller combatants. Since MIO-type operations are

so broadly applicable, they provided a good initial area for the study of NCMW effects. In addition, MIO depend more critically on information and command and control (C2) than on specific weapon systems, which simplifies the problem space and analysis.

In essence, MIO consists of a set of naval forces trying to find and apprehend (possibly deter) targets of interest (TOI) carrying contraband (goods or people). The TOI may be mixed in with legitimate vessels. Typically, the TOI must be identified and apprehended in some specific area so that it cannot pass through that zone and evade the blockade. The required criteria for apprehending vessels can vary, but typically determining whether the criteria are met requires close examination by the interdicting force. These identification processes may require several levels of examination by different units, and may be applied to all vessels or just a sample of them. The task of the TOI is to escape the interdicting force through manoeuvre or deceit.

In MIO, the vessels of interest (or targets) may be regarded as waiting in a queue to be served (or queried, and perhaps inspected and boarded) by warships on patrol. This service also takes time. No two operations are identical, but they are characterised by a sequence of actions starting with a query into the vessel's intent, often followed by a search for contraband by a boarding party, and end in a decision to either apprehend the vessel or allow it to continue.

Collaborative planning and re-planning assumes that dispersed individual commanders, subject to a general commander's intent, can make use of networked communications to develop plans in collaboration as if they were a co-located command. Thus, a MIO force would develop and coordinate its initial plans over the network. The commanders can then make joint decisions on changes to an existing plan as circumstances change. The difference between planning and re-planning is really only one of timing since few plans exist in a vacuum. Planning, however, is often thought of as being an operational level task performed by dedicated command staff, while re-planning in this context is a tactical task.

In both cases, the NCMW application involves doing the normal command staff jobs (for tactical or real-time planning) in a distributed fashion. Thus, while units are dispersed and in the midst of operations, their views and inputs can be obtained for planning or adjusting the operations to adapt to unforeseen circumstances. In a coalition operation, there is a further benefit that all nations and their particular requirements can be included in the plans. Coalition operations are fraught with possibilities for misunderstanding and require that significant effort be put into maintaining relations between the partners. Collaborative planning may provide an additional channel for these efforts, hence the reason for the AG-1 hypothesis.

The expected outputs and results of the use of collaborative planning and re-planning are:

1. improved synchronisation between units since unit commanders understand their partners' parts in the plan and their concerns about the plan
2. increased flexibility in operations because the overall force is able to respond in an adaptive manner to new circumstances
3. improved use and understanding of sensor and intelligence data
4. better matching of force to threat, since units can redeploy to match a threat
5. de-confliction of the battlespace. Since everyone participates in the re-planning, there will be fewer problems of water space or airspace management
6. decreased HQ workload since virtual command teams can be formed outside of the operational level command
7. increased ownership of plans by all units or nations involved since everyone has been involved in the plan development
8. increased speed and quality of command.

The focus of this effort was to investigate the usefulness of applying a queuing model to MIO within the context of the NCMW concept of tactical collaborative planning. Both analytical and simulation-based queuing models were examined, and the theoretical model was applied parametrically to two MIO scenarios.

Using the steady-state probability of target vessel interception (service) as the primary measure of effectiveness, AG-1 was able to demonstrate the usefulness of queuing theory to relate NCMW application measures to force effectiveness. In addition, the queuing models provided valuable insight into the aspects of the MIO task where NCMW concepts might be applied. Thus, the group demonstrated that queuing theory is directly applicable to the second stage of analysis for operations that can be viewed as a demand for service, and provides direction in the process of refining NCMW concepts into testable applications. The parametric results obtained provided general bounds on expected improvements in effectiveness; specific results, however, will depend upon the particular NCMW applications and how they are used.

A complete report of the MIO TACSIT results is beyond the scope of this book but is provided in great detail in the report of the MIO TACSIT Group cited above. The analysis by the MAR AG-1 demonstrated that queuing theory provides a good model for a class of maritime operations that are expected to benefit from

NCMW concepts and applications. Specifically, those operations characterised by a 'demand' for (or avoidance of) service can often be adequately modelled and analysed by applying queuing theory. This fills one of the necessary stages in a quantitative analysis of NCMW concepts - that of linking application measures of performance (MOP) to force measures of effectiveness (MOE).

The examination of engagement level models and the variation of MOE with the parametric study of input MOP is an important part of the process of refining NCMW concepts to the point where they can be tested. The two applications of the NCMW concept of network-based collaborative planning and re-planning analysed by AG-1 using a queuing model highlight the capabilities and shortfalls of the methodology. For aggregate steady-state systems, queuing theory provides a rich source of insight. The analyst must keep in mind however, that in reality, service time and service accuracy often are not stationary processes and interesting phenomena will occur outside of steady-state situations.

The quantitative results obtained from running the MIO queuing models supported the group's hypothesis - that in coalition-force MIO, network-enabled collaboration planning/re-planning could significantly improve the probability of intercepting a contraband vessel in many cases. For example, in a scenario with an overall arrival rate of 25 targets per day, there is a 20 per cent improvement in interception probability simply by providing some mutual coordination within the force, and a 50 per cent increase in capability through dynamic, collaborative re-planning of the force response.[206]

These results confirmed these authors' anecdotal experience from interaction with operators who have participated in MIO in the Arabian Gulf, and thus, this study of coalition MIO provides general evidence to support the continued development of collaborative planning and re-planning applications. Given that a former commander of the US Pacific Fleet noted that 'Maritime interception operations is another maritime-centric effort in our contribution to the Global War on Terrorism and forms perhaps our greatest growth opportunity in our fight against global terrorism', the MIO modelling work conducted by AG-1 should inform coalition partner navies of the substantial benefits of networked operations.[207]

B. Anti-submarine Warfare (ASW) TACSIT

The second tactical situation examined by MAR AG-1 was Anti-Submarine Warfare. Like MIO, it too represented a tactical scenario familiar to all the member nations and one that all believed they would be involved with in the future. The results of this study reported here were extracted primarily from the report of the ASW TACSIT Group at the 9th International Command and Control Research and Technology Symposium.[208]

With significant experience in ASW analysis, AG-1 was able to define the operational and tactical issues at hand and approached the complex issues involved in ASW from a multinational and multilateral perspective with a sound understanding of the challenges and opportunities associated with ASW operations in a coalition environment. The AG-1 team members were armed with literally decades of collective experience in ASW operations gleaned from coalition ASW exercises in various venues, including NATO and the US Pacific Command's Rim of the Pacific (RIMPAC) exercises. Additionally, several of the AG-1 participants were members of the science and engineering staff at the Naval Undersea Warfare Center Division, where they had carefully analysed ASW exercises as part of their ongoing work.

With a far greater background and experience in ASW analysis than with MIO, AG-1 was able to quickly refine the options for this TTCP study and define the way ahead. After weighing a wide range of options regarding what to examine, the group decided to analyse two hypotheses:

1. *In coalition force ASW, network-enabled shared situational awareness (SSA) can reduce false contact loading, by means of data correlation and fusion of the information obtained and provided by individual search elements, and thereby improve search effectiveness.*

2. *Sensor operators in a collaborative information environment (CIE) can reach-back to ASW experts to improve classification performance against both target and non-target contacts.*

AG-1 used two queuing models that incorporate reneging (leaving a queue after entry) and balking (inability to enter a queue) to execute the computations needed to quantitatively analyse these hypotheses.

The rationale for picking these two hypotheses was a desire to move beyond the strong results of the MIO TACSIT and to deal with actions the coalition force might take once it was robustly networked. Thus, while the study did not 'wave away' the issue of robustly linked and networked operations, it attempted to take the analysis to the next level and examine what specific actions would most benefit the force if they were, in fact, robustly networked. After much deliberation, it was determined that shared situational awareness (SSA) and a collaborative information environment (CIE) were two major expected benefits of networking the maritime force. Thus, the ability to support SSA and CIE provided the optimum measures of effectiveness for this analysis. Particular aspects of these benefits were expected to be important for improving the effectiveness of networked coalition ASW and thus were the focus of this study.

Situational awareness means, in essence, knowing what is going on within a volume of space and time. SSA means that two or more individuals understand a situation in the same way.[209] In this study AG-1 examined the possibility of using network-enabled SSA to reduce false contact loading in ASW to increase ASW effectiveness.

A CIE is the aggregation of infrastructure, capabilities, people, procedures, and information to create and share the data, information, and knowledge that enables collaboration among a selected group of individuals or organisations.[210] In this study, AG-1 examined the possibility of using a CIE to connect individual forward-deployed ASW sensor operators with an ASW expert, such as an ashore acoustic intelligence (ACINT) expert, to augment operator expertise, enhance operator performance, and mitigate the relatively poor target versus non-target classification performance of some afloat sonar operators.

The AG-1 team found that the aspects of SSA and CIE, as just described, could be analysed using queuing theory. The team did not suggest that queuing theory was the only effective methodology for examining SSA and CIE, but rather, that for the purposes of this study, queuing theory provided an effective methodology. The group validated the MIO experience that any 'demand-for-service' system, or any system with a waiting line for service that can experience congestion, can be analysed using queuing theory. Therefore, to the extent that a military task or system fits into a demand-for-service framework, it is analysable by queuing theory.

Two queuing model tools, called QDET and QSIM, were used to conduct quantitative parametric analyses of the SSA and CIE ASW concepts.[211] A number of general conclusions were drawn from the analysis that provided evidence of the value of networking ASW forces, and also provided some indication of where network-centric applications might be focused.

The SSA and CIE ASW concepts were conceived, in part, through extensive dialogue with others in the US Navy ASW community, particularly with representatives of the Navy Warfare Development Command and the Program Executive Office - Integrated Warfare Systems. The latter is developing, among other things, a Common Undersea Picture (CUP) capability for US and coalition ASW forces.

The Shared Situational Awareness (SSA) Analysis

SSA means that two or more individuals understand a particular circumstance in the same way. First and foremost, connectivity between distributed systems is needed to achieve this. AG-1 examined the possibility of using network-enabled SSA to reduce false contact loading in ASW, and thereby increase ASW effectiveness. The hypothesis was:

In coalition force ASW, network-enabled SSA can reduce false contact loading, by means of data correlation and fusion of the information obtained and provided by individual search elements, and thereby improve search effectiveness.

Submarines, particularly diesel submarines operating on battery in a complex littoral environment, are difficult to detect, in part because both their passive and active signatures are low. In addition, if contact is gained, it is often held only intermittently. Further compounding the ASW problem is the fact that littoral regions of interest generally contain many false contacts. Thus, false contacts can substantially interfere with the detection of the TOI. More powerful sensors can exacerbate the false contact problem because the number of contacts detected increases approximately as the square of detection range.

There are several 'costs' associated with reacting to false contacts:

1. reactive forces may be diverted or employed unnecessarily
2. fuel, sonobuoys, and weapons may be expended unnecessarily
3. reactive forces may not be available when needed
4. prosecution of real TOI may be delayed or missed.

These adverse events are often observed in real-world exercises. One might ask: to what extent can network-enabled SSA mitigate some of these problems? To explore the false contact problem and test the above SSA hypothesis, an ASW TACSIT was developed. In the case with limited SSA, a Blue forward barrier submarine detects and misclassifies a surface vessel as a TOI and diverts from its planned search track to investigate. This diversion can cause detection of the TOI to be delayed or missed entirely.

In the case with network-enabled SSA, it is assumed that an air platform can provide surveillance of the region of interest and transmit an accurate surface picture to an assumed 'Contact Refinement Node' (CRN). It is also assumed that the Blue submarine transmits information about the suspected TOI to the CRN. The network allows the CRN to be forward or on land. The task of the CRN is to assist with or conduct data alignment, correlation, localisation, and target motion analysis, and classification across sensor contacts and tracks. The CRN shares this information in near real-time with all Blue ASW forces, including the submarine. The result of these activities is that the Blue submarine stays on its intended search track and does not become diverted by the non-TOI, as is the case without network-enabled SSA.

In the model selected, AG-1 needed a realistic estimate of the number of TOIs and non-TOIs that would produce sensor contacts. This number can be considerably larger than the actual number of objects. For given sensor and contact properties

and dynamics, we can then calculate the arrival rate of contacts (customers) to the sensors. The arrival rate (AR) thus comprises the sum of TOI and non-TOI arrival rates.

Some of the TOI and non-TOI are detected by sonar and must be classified. Most of the arrivals are classified easily and are quickly identified as being non-TOI. A portion of the arrivals may be difficult and time consuming to classify as a non-TOI, however, due to the overlap with selected submarine attributes. As a result, detection and classification queues can form in highly cluttered regions.

Added complexities are balking and reneging. Contacts pass into and out of sensor coverage or have some finite lifetime that is often exponentially distributed. If such a loss happens within a queue or within service, then the contact is said to have reneged. If it occurs before entry to the detection and classification processing queues, then the contact is said to have balked.

All of these factors were incorporated in AG-1's multi-contact queuing model. The primary output needed is the probability that an arbitrary contact is acquired and completes detection and classification processing. The probabilities of calling a target a target (a hit or correct classification) and calling a non-target a target (a false alarm or incorrect classification), were then multipliers to the probability of acquisition.

AG-1 analysis of the ASW TACSIT showed that the probability of acquiring a target was a function of contact AR. In the model run, contact AR for the combination of TOI and non-TOI varied from 0 to 10 contacts per hour. In this model, mean time to renege (hold contact) was assumed to be 15 minutes. Curves were produced for mean service times of 15, 30, 60, and 120 minutes, providing a parametric sweep of time to classify a contact by whatever process.

For the SSA ASW TACSIT, this led to the result that, as contact AR increases the probability of acquisition decreases. This occurs because as AR increases, balking and reneging increase. As the queue size grows, some of the possible contacts balk because they cannot enter the queue, and some of the contacts in the queue renege because they take too long to be serviced.

One effect of SSA is to decrease the AR of non-TOI to the classification system. There are several possible ways this can occur within SSA, for example, by surveillance of a portion of the non-TOI field, as previously described. It can also occur by the use of sophisticated Tactical Decision Aids (TDA) that can correlate some sensor contacts with non-TOI objects or phenomena (such as reverberation prediction with active sonar).

Thus, the AG-1 modelling showed that the decrease in the AR of non-TOI does result in a higher probability of acquisition against the TOI. This effect of improved

SSA, yielding a higher probability of acquisition can be parametrically analysed. This exemplifies the value of SSA on reducing contact AR, and in turn, increasing ASW effectiveness.

The principal findings of this study of SSA on false contact loading in ASW were as follows:

1. Queuing theory can provide a framework for the analysis of the SSA ASW concept, because SSA is a 'demand for service' process.
2. Improving classification performance against both benign contacts and targets of interest can increase ASW effectiveness. In effect, this reduces the arrival rate of benign contacts, thereby increasing the probability of acquiring targets of interest.
3. An accurate surface picture, shared among the ASW units, could improve ASW effectiveness. Networking the force for information transfer is a key enabler of this aspect of SSA. Real-time connectivity is needed.
4. An alternative method for increasing ASW effectiveness is to employ more ASW units, that is, increase the number of servers.
5. The queuing theory framework can be used to analyse the trade-off in benefits between shared information and force size (that is 'bits' versus 'bangs').

In this section, we examined the possibility of using network-enabled SSA to reduce false contact loading in ASW to increase ASW effectiveness. The AG-1 hypothesis was: *In coalition force ASW, network-enabled SSA can reduce false contact loading by means of data correlation and fusion of the information obtained and provided by individual search elements and thereby improve search effectiveness.* AG-1's findings provide quantitative evidence that supports this hypothesis.[212]

The Collaborative Information Environment (CIE) Analysis

A CIE was defined above as the aggregation of infrastructure, capabilities, people, procedures, and information to create and share the data, information, and knowledge that enables collaboration among a selected group of individuals or organisations.[213]

AG-1 examined the possibility of using a CIE to connect individual forward-deployed ASW sensor operators with an ASW expert, such as an ashore acoustic intelligence (ACINT) expert, in order to mitigate the relatively poor target versus non-target classification performance of some sonar operators. The team also

examined the possibility of using network-enabled CIE to improve the overall ASW classification performance and effectiveness of forward-deployed force elements. The hypothesis was: *Sensor operators who did not have the requisite expertise to succeed at this target classification challenge in a CIE can reach-back to ASW experts to improve classification performance against both target and non-target contacts.*

Once sensor contact is made on an object or phenomenon, the detection and classification problem is, in essence, an analysis and decision-making problem. There are many determinants of decision-making behaviour, including:

1. problem complexity
2. time available
3. number/quality of alternatives
4. perceived risks
5. information presentation rate
6. individual differences in cognitive and decision styles
7. level of expertise.

A small percentage of sonar operators have great expertise and are considered experts at what they do, for example, ACINT riders on ASW platforms. Therefore, it might be possible to use the network, with additional infrastructure, to link sensors, operators, experts (not collocated with forward operators), and TDA to improve ASW performance. This concept is an extension of the reach-back cell (RBC) concept. The RBC normally provides:

1. environmental assessment
2. sensor performance predictions
3. red-cell wargaming
4. initial ASW battlespace assessment
5. initial plans, including unit stationing, tactics, and sensor employment
6. submarine contact database management
7. submarine contact information fusion
8. ongoing analyses and assessments of mission execution
9. sensor/threat experts to advise forward operators, if needed.

With robustly networked coalition forces, forward sensor operators *can* be linked to an ASW expert. In fact, multiple operators can be forward and linked by means of a connectivity infrastructure to an expert threat analyst and sensor operator. The operators and expert can be considered as being embedded in a CIE. The expert would usually respond to requests for assistance by the operators. Due to the nature of ASW, including the problem that holding time may be short; the CIE requires synchronous tools to allow collaboration between simultaneously engaged participants. In addition, the expert will need to be aware of the ASW context and history experienced by each operator. This amount of information can be used to define the network architecture and the characteristics of network infrastructure.

Using some of the same parameters of the SSA case above, AG-1 determined quantitatively that the probability of acquisition of a contact was enhanced when the forward-deployed sonar operators were able to operate in a CIE. The group found, as might be expected, from the larger number of variables in the 'equation' (expertise of the individual sonar operators, expertise of the ACINT expert, type of target submarine, type of shipboard and/or aircraft equipment, etc.) definitive numerical results were not as readily available as in the SSA case. Nevertheless, the available evidence and the analysis showed a strong correlation between the degree of CIE established and ASW success - suggesting that more detailed analysis in this area is warranted.

The principal findings of this study of CIE on ASW effectiveness are as follows:

1. queuing theory can provide a framework for the analysis of the value of the operator-expert CIE because this collaboration is a 'demand for service' process
2. networking the force can enable a CIE that, through improved classification performance, might increase ASW effectiveness
3. synchronous collaborative tools are needed to enable this collaboration
4. expert workload may need to be controlled to avoid 'missing' requests for assistance.

In this work, AG-1 examined the possibility of using network-enabled CIE to support operator - expert collaboration in order to improve ASW classification performance and effectiveness. The hypothesis was: *Sensor operators in a CIE can reach-back to ASW experts to improve classification performance against both target and non-target contacts*. The findings provide evidence that supports this hypothesis.

Summary of the ASW TACSIT Analysis

In this study AG-1 showed, through the analysis of two ASW TACSIT, that network-centric concepts can enable SSA and a CIE. Both SSA and operator - expert collaboration in a CIE were shown to improve ASW performance and effectiveness. Specific warfighting findings included:

1. ASW effectiveness can be increased by improving classification performance against both benign contacts and targets of interest. In effect, this reduces the arrival rate of benign contacts, which thereby increases the probability of acquiring targets of interest.
2. An accurate surface picture, shared among the ASW units, could improve ASW effectiveness. Networking the force for information transfer is a key enabler of this aspect of SSA. Real-time connectivity is needed.
3. Networking the force can enable a CIE that, through the increase of classification performance, would likely increase ASW effectiveness. Synchronous collaborative tools are needed to enable this collaboration.

The results from this analytic effort indicated that selected NCMW ASW concepts, if implemented, should have positive effects on ASW effectiveness. For example, NCMW applications that decrease the mean time to service contacts, in general, improve effectiveness. Furthermore, applications that decrease the arrival rate of unwanted contacts can improve the detection and classification of ASW targets of interest.

Anti-Surface Warfare/Swarm (ASuW/Swarm)

The third and final TACSIT examined was that of ASuW operations, specifically 'Swarm' attacks against coalition naval units. In many ways, this TACSIT represented the most interesting and challenging case studied by AG-1 for a number of reasons. First, for the MIO and ASW cases, the coalition force would be primarily on the 'offensive' against either ships with contraband or hunting enemy submarines (although there clearly is a strong defensive component to many ASW operations), while in the Swarm case the coalition naval force would definitely be on the 'defensive'. Second, in the MIO and ASW cases there was typically a slow-moving tactical problem, while in the Swarm case, the tactical situation was one that moved rapidly. Finally, this Swarm case was one that lent itself to the use of a completely different model than those used in the MIO and ASW TACSIT, thus ploughing new ground for analysis.

The results of this study, reported here, were extracted primarily from the report of the ASuW/Swarm TACSIT Group at the 10th International Command and Control Research and Technology Symposium.[214] Because this 'warfare domain' is relatively new, some additional background explanation of the nature of the challenge is in order.

In the ASuW problem in general and Swarm attacks in particular, battlespace control near land is essential to ensure prompt access and freedom of manoeuvre for coalition forces moving from the sea to objectives in the near shore area. As coalition naval forces operate in littoral areas, potential adversaries are responding with innovative, often asymmetric approaches to coastal naval warfare. A number of coastal nations - several of which border strategically important waterways - are exploiting small boat warfare and integrated coastal defences to blunt, neutralise, or defeat larger navies operating in the near shore area.

The tactic that appears to have the most traction with these nations is that of 'swarming' attacks by large numbers of fast inshore attack craft (FIAC). There is no simple definition for these craft - they can be as small as recreational vehicles such as a jet ski or as large as naval or coastal fast-patrol boats. 'Swarming' attacks can also come from multiple axes and use various attack formations. The navies of coalition nations have conducted numerous studies and analyses to grapple with the threat of swarming small boat attacks. In one study for the US Navy, an industry team found that different types of threat platforms had different effective weapons ranges. The study grouped these into two general categories: small threat platforms (cigarette boats, Boghammars, and others) with a maximum effective weapon range from 0.1 to 0.5nm (Type 1) and larger naval vessels such as advanced patrol boats carrying short-range guided missiles (Type 2 / Type 3).

While a number of studies did not discount 'swarming' attacks by larger vessels such as advanced patrol boats, the studies focused heavily on swarming attacks by very small craft as the predominant scenario likely to be faced by coalition navies operating in littoral waters. The consensus of a number of studies and the opinions of serving naval officers appear to converge and focus on a primarily massed small boat threat consisting of 10 to 20 high-speed manoeuvring boats attacking over a 20 to 60 degree azimuth sector. The boats have a simultaneous arrival time with closing speeds of up to 35 knots. Their manoeuvre is typically in a sinusoidal path. The small boats are considered to be commercial types with no obvious distinguishing feature to support easy classification. Identification of an attack results from the characteristic behaviour of a large number of high-speed inbound boats.

The threat of swarming small boats is not a new one. For a number of years, work in naval laboratories focused on the small, fast, manoeuvrable boats as primary threat elements. The operational experience of serving naval officers in AUSCANNZUKUS

nations indicated that naval forces must be capable of engaging small coastal naval combatants such as patrol boats and guided missile corvettes or other smaller boats. Several reports noted that boats could be operated unpredictably and under unexpected conditions. These reports concluded that these craft may appear as part of the normal friendly or neutral traffic in an area, making them all the more difficult to counter. In addition, industry reports provide numerous examples of observed and reported naval exercises by hostile nations that demonstrate their willingness and ability to surreptitiously get inside the effective maximum range of the surface weapon systems of a larger naval force.

The nature and the magnitude of this threat have riveted the attention of coalition navies who recognise, in general, that a coordinated response from networked coalition naval units is the optimal way to defeat this threat. In a 2002 article in the US Naval Institute *Proceedings*, a future US Chief of Naval Operations - then Vice Admiral Michael Mullen - noted that:

> Small, fast enemy surface combatants represent another threat to operations in geographically confined areas, where their size and the surrounding clutter of geography and traffic make long-range detection difficult…A diverse force, networked with distributed sensors, offers promising response capabilities once enemy vessels are under way.[215]

While this swarming small-boat attack threat has been discussed in professional journals and reviewed in depth in various studies, there has been, to date, little quantitative analysis to determine the extent to which networking coalition naval platforms can help to deal with such a threat. Therefore, it was determined that this was a particularly fruitful area for AG-1 analysis.

The AG-1 ASuW/Swarm study characterised the degree of networking between members of a maritime force, and used the map-aware non-uniform automata (MANA) intelligent-agent-based distillation model to represent the C2 and sensor interactions between allied units, and separately between the units of the attacking force. The study sought to determine what degree of improvement was possible via surveillance and targeting and indicated the point at which the battle must be moved 'offshore' using either helicopter or unmanned combat air vehicle (UCAV).

The AG-1 challenge was to investigate possible network-centric measures to overcome the Swarm threat, using operational analysis to quantify the outcome. The problem was defined by very short surveillance (detection) ranges due to the small size of Type 1 FIAC, and even shorter identification (ID)/classification range.[216] These factors are very scenario/environment dependent, and ducting conditions may hamper ship-mounted sensors. Such factors, plus current rules of engagement, ensure that engagements are now conducted at 'whites of the eyes' ranges well inside potential enemy weapon launch range.

The FIAC/Swarm study was initiated in early 2003 (and completed the following year) and AG-1 took a broad three-level modelling approach using the following tools:

1. 'simple' spreadsheet, plus the Queuing Theory (QT) models
2. MANA model
3. Threedim model.

The platforms likely to be involved in the modelling included some-high value units; their escorts, typically one or two destroyers or frigates (DD/FF); some airborne assets (helicopter or unmanned aerial vehicle (UAV)); the opposing forces; and background or neutral shipping. The 'three-tier' approach was to provide depth and a degree of validation and verification; it was not clear at the outset whether the spreadsheet and QT models might (through meta-modelling) over-simplify the problem. However, there was some confidence in MANA's strengths as an intelligent agent model to represent swarming aspects, while Threedim (as a fully featured battle model) had the ability to model at greater fidelity, including weapon system arcs, but with a simpler (such as a 'dumb') target set.

A modelling workshop was held in late 2003. The characteristics of FIAC and defensive systems were presented and discussed along with the operational realities of Swarm engagement, using experts from the UK Maritime Warfare Centre at HMS *Dryad*. The study hypothesis was reviewed and it was agreed that it captured the essence of the analysis problem:

> *In an ASuW Swarm attack, Blue force shared situational awareness and an associated sensor-to-effector capability reduces the number of leakers against Blue force assets.*

The NCMW options for the FIAC/Swarm study include the following cases, with varying degrees of 'networking':

1. Baseline. No communications or networking between units. This is not realistic, but sets the base case for proper comparison between options, by reducing the force to a collection of 'singleton' ships that cannot act in a coordinated manner.
2. Low. Shared situational awareness but with organic targeting.
3. Intermediate. Shared situational awareness and organic targeting (as Low case), plus reach back to intelligence information.
4. High. Shared situational awareness, organic targeting, and reach-back to intelligence information (as Intermediate case) plus inorganic (for example, off-board) targeting.

Accurate metrics and presentation of results, demand suitable measures of effectiveness to determine the effect of NCW in the Swarm attack scenarios. The following MOE were adopted:

1. the fraction of Red force threats that come within their weapons range of the high-value unit (HVU)
2. the probability of at least one Red force threat reaching its weapons range of the HVU
3. the number of naval vessels that suffer defence capability-kill while defending the force
4. the number of neutrals inadvertently destroyed, (only relevant when inorganic weapons targeting is used).

The results were generally presented as graphs of the probability or number of leakers versus the weight of attack. Where available, the standard errors in the average MOE value were used to provide uncertainty estimates for them.

During the initial modelling work, the base case results with point defence and improved target indication (TI) for a single-sector attack (using close-range guns and various permutations of gun range and slew times), showed that:

1. current point defence systems can be overwhelmed by a relatively small number of FIAC
2. the key drivers are FIAC speed, rate of Blue weapon fire determining the number of shots before Red fires, and the effective range difference of Red and Blue weapons.

The results of the three models were in substantial agreement and AG-1 decided to use MANA as the principal model to analyse Swarm attacks for the remainder of the study. This book will move directly to the general results of the analysis as the full results of this MANA model work are classified because of the sensitivity of the models and the work involved.

The analysis pointed to a number of operational benefits derived from robust networking. The broad classes of operational gain from 'network enabling' forces, when compared to the baseline 'singleton' case are:

1. Better use of close-range guns. This is achieved by meeting the rules of engagement criteria for opening fire at the maximum useful weapon range, rather than a shorter range, once decisions have been made by each weapon crew and ships command team. This applies to manually aimed ('crew served') weapons like the M-60 machine gun or 40-mm grenade launcher, and 20-mm and 30-mm cannon, as well as autonomous weapons like Phalanx Block 1B.

2. Use of medium-calibre gun to maximum range. The escorts' medium calibre gun (a US 5"/54 or the UK 4.5" Mk 8) will typically fire 20 to 25 rounds per minute out to about 26km, with either direct action (DA) fusing (exploding on impact with the sea or a target), or via a variable time (VT) proximity fuse for airburst over the target, which is attacked by the shell fragments.

3. Move the battle outwards. This is accomplished by using helicopter or UCAV. This class of benefit applies to all classes of FIAC and provides either ISR/ID information about the target, thus achieving engagement criteria for ship mounted weapons, or the helicopter or UCAV can also be armed and then used to attrite the incoming FIAC raid. The differences are that the crewed helicopter can be autonomous, while the UCAV relies on good networking with the controlling ship.

The results of the analysis using the MANA model clearly showed the need to 'do something'. Present ships' defences are sensor-limited by short detection and ID ranges, and are sometimes hampered by restrictive rules of engagement. Saturation therefore can occur at relatively low weights of attack by Type 1 FIAC.

An ASuW Swarm could be countered by networking between escorts, helicopters/UAV/ UCAV and the merchant ships. Improvements come in three broad bands:

1. Use of existing close-range guns (machine guns, 20/30-mm, Phalanx 1B) to maximum range, to defeat Type 1 threats.

2. Use of existing medium-range weapons to medium-range bracket to attack Type 2 FIAC, plus use of smart rounds (laser designator in helo/UAV) to maximum range.

3. Maximum use of armed helicopters/UCAV to attrite raids farther out. This is the only counter to a longer range Type 3 attack, but the trade-off between helo and UAV/UCAV depends on the scenario.

The results of the AG-1 MANA analysis showed that for the smallest Type 1 FIAC, intermediate and high levels of networking could increase force survivability substantially. Countering the larger Type 2-3 FIAC could be achieved by the use of networked air ISR.

The trade-off between helicopter and UCAV depends on whether the threat adopts a single sector or widespread (such as isotropic) attack. Armed airborne assets will always improve the survivability of the force, but the finite weapon payload and space/time considerations caused by the target spread, drive the number of airframes required.

In summary, the third and final MAR AG-1 TACSIT showed, as its two predecessors did, that robust coalition networking could provide substantial benefits. In this case,

it increased the probability of success when a naval force is attacked by a FIAC 'Swarm' attack. The nature of the study organisation and the fidelity of the MANA model also informed the study team of specific tactics that could aid the defending force in fighting off such an attack. Accordingly, the ASuW/Swarm TACSIT was an important outcome of AG-1's work and a valued input for the work of AG-6.

As indicated earlier, AG-1 was chartered for a defined period of time, October 2001 to September 2004. The TTCP methodology and 'rules of the road' are for an action group to complete its work in two to three years, report out to its governing body (in this case, the MAR leadership), and then dissolve. Based on this remit, AG-1 completed its work on schedule and passed its body of work on to the MAR and TTCP leadership.

When the AG-1 Chairman reported on the group's work to the MAR leadership, that leadership team determined that the issue of coalition networking was so important that it wanted this work to continue. The MAR leadership decided that the best way to leverage the work of AG-1 and to explore new challenges was to charter a new group, AG-6, and direct this group to extend the work of AG-1 to a greater degree of specificity with respect to systems and processes required to implement network-centric maritime warfare.

Roughly concurrently, the US Navy decided to make a major capital investment in FORCEnet as the systems that would 'network' the US Navy at sea. Therefore, the MAR leadership directed the stand-up of a new action group to focus specifically on the impact of coalition partners - the four Commonwealth nations - working with the US Navy in a FORCEnet environment. The new action group was tasked to study 'FORCEnet Implications for Coalitions'. Terms of Reference (TOR) were quickly issued and the work of AG-6 began.

Action Group 6 (AG-6) FORCEnet Implications for Coalitions

Based on a strong recommendation by the MAR leadership for a 'seamless handoff' from AG-1 to AG-6, the two teams met together in late 2004. This was a closeout meeting for AG-1 and a start-up meeting for AG-6. Three AG-1 National Leaders transitioned from AG-1 to AG-6, ensuring much of the continuity and leveraging off effort that the MAR leadership sought. Additionally, there were members of other delegations that continued from AG-1 to AG-6. There was a significant change to the US team. But the ultimate result was a team ready to undertake new challenges, while retaining the collective benefit of first-person, detailed knowledge of the AG-1 studies, as well as the experience of working in an intense coalition environment.

Based on the knowledge that AG-6 would not take long to 'get up to speed', the MAR leadership set in place an aggressive schedule to complete the work. The MAR TOR directed:

> Building on the results and findings of AG-1, MAR initiated plans for a follow-on 'FORCEnet Implications for Coalition' Study (AG-6) to examine the implications and way ahead for realizing coalition capabilities that are compatible with both the functionality and timeline of the US Navy's FORCEnet initiative. (MAR leadership seeks to) define in functional terms various levels of coalition interoperability with FORCEnet; to assess the incremental value of higher levels of interoperability; to make appropriate use of USN FORCEnet and other TTCP nations' systems engineering effort, of TTCP nations' modelling capability, of interactions with Trident Warrior and other exercises, and with other TTCP Group efforts, (e.g. HUM); and provide input to national balance of investment studies.[217]

When the MAR leadership stood up AG-6 and directed it to leverage the work of AG-1, there was a built-in mandate for continuity and, as mentioned above, some AG-1 members, including three national leaders, transitioned from AG-1 to AG-6. However, on the US team, there was an almost complete turnover of personnel. This occurred because, with the shift in the new group's focus to FORCEnet, there was a concomitant mandate for change to bring sufficient subject-matter expertise to the team. Accordingly, the new US National Leader and several team members were drawn from the Space and Naval Warfare Command (SPAWAR) in San Diego (then the US Navy's FORCEnet Chief Engineering entity) and from that command's principal laboratory, SPAWAR Systems Center, San Diego (SSC San Diego - now SSC Pacific).[218]

Some additional background is needed to understand the importance of this transition. The SPAWAR Enterprise had been at the forefront of FORCEnet development since the concept evolved from the work of the US Chief of Naval Operations' Strategic Studies Group a number of years ago. Soon after Admiral Vern Clark took over as the US Navy's CNO, he articulated the US Navy's vision as 'Sea Power 21' based on the four pillars of Sea Strike, Sea Shield, Sea Basing, and FORCEnet.[219] While some critics considered the first three pillars as another variation of an old theme, most seasoned naval observers recognised that FORCEnet was indeed something new and exciting that could fundamentally alter the way naval warfare was conducted.

The detailed vision for FORCEnet was set forth in a 2005 publication of the Naval Network Warfare Command's Capstone Document, *FORCEnet: A Functional Concept for the 21st Century* (NNWC Capstone Document). Signed by the Chief of Naval Operations and the Commandant of the Marine Corps, this short document

defined the importance and essence of FORCEnet and explained where FORCEnet would fit in the overarching context of military command and control. Importantly, the publication provided the US Navy's working definition of FORCEnet:

> FORCEnet is the operational construct and architectural framework for naval warfare in the Information Age, integrating warriors, sensors, command and control, platforms, and weapons into a networked, distributed combat force.[220]

In straightforward terms, FORCEnet referred to the systems and processes for providing fully networked naval command and control from 2015 to 2020. The objective of FORCEnet was to provide commanders the means to make better, timelier decisions than they currently can and to allow the effective execution of those decisions. The concept envisioned extensive connectivity among network elements - greater by orders of magnitude than previously achieved. Since most headquarters are already well connected, the real power of FORCEnet was to be in connecting the extremities of the force - people, weapons, sensors, platforms and other entities, ultimately extending visibility and empowerment to the extremities.[219] The development of FORCEnet, like the development of the Global Information Grid (GIG) itself, followed the precepts of the CCRP, in making FORCEnet the *naval* portion of the GIG.[222]

The NNWC Capstone Document described 15 required FORCEnet capabilities that guided the technical community in designing FORCEnet to enable warfighters to achieve the maximum utility from this system. While a listing of these 15 attributes is beyond the scope of this book, they are available for ready reference in the NNWC publication.[223] Importantly, AG-6 examined the publication and determined that these attributes were consistent with the kind of naval command and control that all nations desired.

Within SSC San Diego, scientists and engineers had been working on FORCEnet since its inception, and they soon discovered the FORCEnet design parameters enabled them to do some interesting things. They learned that the totality of the US Navy's 'higher level guidance' on FORCEnet, ranging from the initial concept documents produced by the Chief of Naval Operations Strategic Studies Group to SPAWAR Headquarters' FORCEnet Architecture and Standards document,[224] allowed them a wide range of ways to actually *design* FORCEnet as it would be deployed to the US Navy fleet.[225]

Using its extensive background in navy networking at sea, command and control, knowledge management, human systems integration, and other disciplines, this SPAWAR Headquarters and SSC San Diego team devised an approach to the design of FORCEnet that SSC San Diego dubbed 'Composeable FORCEnet'.[226] The viability of this approach has been recognised by the Office of the Assistant

Secretary of Defense for Network Information Integration (ASD NII) in its 2006 publication *Understanding Command and Control*,[227] as well as by the Department of the Navy Chief Information Officer in the Department's 2006-07 Strategic Plan.[228]

Armed with this 'model' of Composeable FORCEnet as a guide, AG-6 set to work immediately to carry out the mandate of the TOR and to 'bound the problem space' to work through the issues of coalition interoperability in general and the issues of coalition nations falling in on the US Navy's FORCEnet capabilities. The aim of the effort was to zero in on the TOR remit and 'harmoniz[e] national coalition C4I interoperability strategies and development plans'.

MAR AG-6 and its predecessor AG-1, sustained an analytical effort for over six years (2001-08) examining maritime network-centric warfare and FORCEnet implications for coalitions. These teams generated metrics that show how much more effective a networked coalition maritime force is over one that is not networked. AG-6 generated analytical data and conducted modelling and simulation to demonstrate that if the US Navy's FORCEnet is developed in a way that is inclusive of likely coalition partners, who, in turn, build their national systems to be compatible with FORCEnet, the naval forces involved will enjoy a quantum increase in capability.[229]

AG-6 took the MAR TOR and developed three premises and a hypothesis to inform its work. The first premise, derived from the NNWC Capstone Document, was that FORCEnet will empower warfighters at all levels to execute more effective decision-making at an increased tempo, which will result in improved combat effectiveness and mission accomplishment.[230] The second premise, derived directly from the MAR TOR, was that the warfighting benefits of FORCEnet in a coalition context can be assessed through analysis and quantified to provide input to national balance of investment studies of the five member nations. The third premise, derived from the US Navy Fleet Commanders' top C4ISR priorities, was that FORCEnet had to address current and near term information system requirements that support operations in the joint and coalition environments. *Coalition Communications was the clear number one priority* of all numbered fleet commanders and is a critical enabler in leveraging coalition partners in the global war on terrorism.

Based on these premises, AG-6 developed a working hypothesis that informed its work from the outset. This hypothesis, '*Conducting modelling and simulation and detailed analysis to demonstrate the enhanced warfighting effectiveness of coalition partners (in this case – the AUSCANNZUKUS nations) netted in a FORCEnet environment can help inform national naval C4ISR acquisition programs*', not only set the tone for the group's work, but also provided visibility throughout the naval and defence establishments of all five member nations regarding the group's efforts. The compelling nature of this hypothesis has caused

other organisations not initially involved in AG-6's work to 'jump on board' and join this team.

Armed with effective premises and a working hypothesis, AG-6 constructed a study plan process adapted from the Navy Warfare Development Command. The study plan began with goals and objectives, moved through problem characterisation, then through an innovation and experimentation continuum, through venue selection and an analysis assessment and finally to deliverables; FORCEnet alignment requirements to guide the five nations' acquisition programs. Selecting a tried-and-true study plan process bounded the problem space for AG-6 and accelerated the group's progress.

AG-6 deliberated for some time in order to find a scenario that represented a real-world naval challenge and one that also lent itself to the kind of detailed analysis necessary to address the TOR requirements of the group. AG-6 ultimately determined that a scenario that caused a coalition naval force to conduct not just one - but multiple, cascading missions - would both mimic real-world conditions and present robust possibilities for analysis.[231]

The scenario selected involved coalition naval operations in and around the South China and Philippine seas. In this notional scenario, a coalition naval force initially is tasked to provide humanitarian support and disaster relief in a Southeast Asian nation. When indigenous separatist groups use the opportunity afforded by this chaos to foment trouble, the humanitarian support and disaster relief mission quickly morphs into peace-making/peace-enforcement. As the scenario evolves, the coalition naval force ultimately faces a challenge from a neighbouring nation unhappy that this force is on scene, and the coalition naval force ultimately must deal with surface and submarine threats.

The group determined that selecting the right mix of naval vessels to undertake these missions was just as important as picking the right scenario to use in the study. After extensive dialogue with uniformed naval professionals in all five nations, a decision was made that a naval force built around a US Expeditionary Strike Group (ESG) with supporting ships and aircraft from the other four nations, would represent the most realistic coalition battle formation for this mission.[232]

A summary of the full scope of AG-6 efforts is presented below. AG-6 analysed the extent that coalition networking built on leveraging the US Navy's FORCEnet (Fn) capability would enhance the chances of mission success. The levels of interoperability selected for analysis were:

Option 0	(do nothing)	Small size (all US) ESG force, fully Fn capable
Option 1	(do minimum)	Added coalition ships, but not Fn capable (larger overall force)

Option 2	Intermediate Fn capability to the additional coalition ships
Option 3	Full Fn capability to entire force – robust networking

Then, four principal measures of effectiveness - time to capability (number of major amphibious units delivered on time in the area of operations), economy of effort (cost of munitions, fuel and other consumables used in the campaign), risk (Blue force attrition in all phases of the campaign: assembly; littoral transit; anti-submarine warfare; anti-surface warfare; anti-air warfare; offload; naval fire support; and mine warfare), and campaign success (success in the aforementioned campaign phases and ultimately, the safe delivery of 'campaign effectors' the landing force ashore) - were devised to measure the effectiveness of a robustly networked coalition force that fully leveraged the US Navy's FORCEnet capability over one that was not networked.

Concurrently, the AG-6 members liberally shared the 'technology on-ramps' of their acquisition communities to find those windows where similar technological capabilities could be inserted into their naval C4ISR systems. By modelling the planned capabilities of these 'on ramps' against the scenario, the impacts and value of alternative coalition network structures was assessed. The resulting analysis was presented to MAR principals in 2008 and is currently being used by AG-6 members to make detailed communications technology procurement recommendations in their respective countries.

The advantages that can accrue to the world's peace-loving nations by leveraging the tremendous investment the US Navy is making in FORCEnet cannot be overstated. Far from a US Navy-only standard, FORCEnet - and especially a currently-fielded prototype called 'Composeable FORCEnet' - is a publish-and-subscribe system based on open architecture and open standards that other nations can leverage with minimal investment.[233] An analogy familiar to many, especially in the Pacific Rim, involves Singapore. In 1998, Singapore made an enormous investment in the Singapore ONE project, which provided broadband infrastructure of high capacity networks and switches, with the goal of providing broadband access to the entire nation.[234] Singapore then went out to the international business community and said, in essence, 'Come join us. We have made the investment in building a world-class infrastructure. This is a great home for your business'. Attracted by that world-class infrastructure, those businesses did come, and Singapore's standing as a hub for international business and as a strong node in the Asian economy is a matter of record.[235] The question for AG-6 was whether FORCEnet could play a similar role in the development of maritime coalition capabilities.

The reviews of TTCP MAR AG-6's work within the naval and defence establishments of the five nations have been overwhelmingly positive. Within the US Navy, in particular, one measure of the group's success is the number of organisations outside the naval laboratory and acquisition community - the Office of Naval Research, the Naval War College, the Naval Postgraduate School, and others - who placed members on the team because they recognise the importance of its work.

Importantly, while TTCP represents the work of only five nations, and the MAR AG-1/AG-6 effort represents only a small fraction of the entire TTCP body of work, it must be noted that the issue of coalition networking is sufficiently compelling and the TTCP process sufficiently worthy of emulation, that those outside the TTCP network have identified this as a best-practices example and argued for similar efforts to be conducted by other national groups. In a *Naval War College Review* article, Commander Alberto Soto, Chilean Navy, put it this way:

> Since 2002, the Technical Cooperation Program … has focused the efforts of its Maritime Systems Group (MSG) on 'Networking Maritime Coalitions' and 'FORCEnet and Coalitions Implications.' The MSG has become an important link among national naval C4ISR acquisition programs … For that very reason these [Latin American and Caribbean nations] should tenaciously strive to become involved in initiatives like MSG.[236]

With this look at what TTCP MAR AG-1 and AG-6 groups have accomplished, it is time to turn to the all-important issue of harmonising national C4ISR technology acquisition programs in ways that enhance coalition networking.

Extrapolating the TTCP model to other nations - a bridge too far or a worthy undertaking?

As we suggested at the outset of this book, the ultimate solution to achieving near-seamless interoperability among nations seeking to secure the global commons in global, regional, or more local maritime partnerships is to have the navies of *all* participating countries work together at the laboratory level to harmonise their naval C4ISR purchases.

As Commander Soto has suggested, other nations and navies can leverage the policies and processes that TTCP has instituted among the five AUSCANNZUKUS nations to other groups of nations and navies in natural clusters, so they can begin to replicate the TTCP model where it makes the most sense. As he suggests, the navies of South America offer one such grouping. The ASEAN nations offer another potential grouping and one that already has several collaborative forums. NATO

offers another, and given the wide range of similar efforts already underway such as the NATO Network Enabled Capability (NEC) C2 Maturity Model, this may be easier than some think.

Taking the Next Steps: Harmonising National C4ISR Technology Acquisitions

The TTCP model continues to provide a means for the laboratory communities in the five nations that will likely work together at sea to analyse technical communication and networking needs in an operational framework. The application of the TTCP model to current and future efforts to build effective coalition communication networks can be an important step in enabling Commonwealth nations and the nations they are most likely to partner with to operate and cooperate at sea in this century.

It is important and necessary to use work such as TTCP as a means to harmonise national C4ISR acquisition programs because the challenge is so great. This challenge has persisted for quite some time, as pointed out over a decade ago in an analysis of Operation JOINT ENDEAVOR in Bosnia where it was noted:

> Coalition operations such as Joint Endeavor present a complex set of challenges for the military C4ISR systems planners, implementers, and operators. The most difficult challenge is the provision of integrated C4ISR services and capabilities to support the needs of ad hoc multinational military force structures and politically driven command arrangements. Although integrated C4ISR services are the desired objective, the realities tend to drive the solution to stove-piped implementations. In spite of technology advances, this will likely be the case for some time to come. There will continue to be uneven C4ISR capabilities among coalition members who will continue to rely on systems with which they are most familiar – their own.[237]

But there is reason for optimism because in the decade-plus since JOINT ENDEAVOR, progress has been made in this area, beginning with a more robust and well-nuanced understanding of the challenges involved in this all-important effort. This is especially important from the perspective of Australia and the sea change in Australia's strategic doctrine.

As McCaffrie and Rahman point out in their *Naval War College Review* article, the shift in focus between Australia's previous strategic doctrine, the defence of Australia and the strategy set forth in the 2009 Defence White Paper is striking. While the defence of Australia doctrine, as the name implies, 'adopted a minimalist approach to defence strategy, with an emphasis on denial capabilities in the so-

called sea-air gap to the immediate north to prevent any physical attack against the continent itself',[238] the 2009 Defence White Paper calls for a more maritime-focused strategy and one that appears to place more of a premium on regional and international cooperation, especially between the RAN and other navies.

The reasons for this change in strategy are attributed to a host of factors and need no repeating in this book. This means that Australia in general and the RAN in particular (the force structure of which is clearly a major beneficiary of this new doctrine committing to a more deployable force) must be able to network more effectively and routinely with regional navies and periodically with other navies globally. Robust and effective networking capability is no longer a luxury - it is an absolute requirement.

Not surprisingly, Australia's maritime doctrine is clearly aligned to support this requirement. As pointed out in Chapter Three, but worth repeating here, the capstone publication, *Australian Maritime Doctrine*, refers to the requirement to harmonise naval C4ISR acquisitions this way; 'The greater the commonality of equipment and methods achieved, the less duplication of resources and fewer delays there will be in achieving operational results when nations come together in contingencies'.[239] This is reinforced in *The Navy Contribution to Australian Maritime Operations,* which notes; 'These systems [wide area command and control tools such as secure web-based chat rooms and information exchange systems] have become fundamental to Coalition force operations since the beginning of this decade and are currently being fitted into all RAN surface combatants'.[240]

And this imperative has been reinforced in more recent publications that represent, collectively, the view that the RAN must continue to be a leader in promoting and enabling effective coalition networking. For example, from Sea Power Centre - Australia's perspective, Andrew Forbes and Captain Peter Leavy, RAN, note:

> At the operational level of engagement the RAN is regularly involved in a large number of international exercises and operations… These activities are critical to the development and maintenance of mariner and *interoperability skills, along with practicing combined command and control arrangements necessary to operate in effective coalitions*. [emphasis added].[241]

Clearly, Australia faces an additional challenge based on its regional responsibilities. In addition to partnering with larger navies such as those of other nations as well as the United States, Australia, for reasons of geography, tradition, and real-world contingencies, often finds itself partnering with smaller - often substantially smaller - navies of the Oceania and Southeast Asian region. As Chris Rahman points out in *The Global Maritime Partnership Initiative*, 'Technical impediments to information sharing can embrace a range of factors…Developing the capacity of small navies

and developing countries to successfully incorporate the [C4ISR] technology can be somewhat more difficult'.[242] The duality of Australia's role - as a global partner to large navies and a regional partner to smaller navies - makes it natural that Australia takes a leadership role in networking the global maritime partnership.

While some might contend that putting something in strategic documents does little (or nothing) to contribute to coalition networking, we contend that this is an absolutely vital first step to influencing national acquisition authorities to acquire the appropriate 'kit' to enable navies to network effectively when they work together to secure the global commons. As Dr Norman Friedman points out in *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars*, 'Overall, networking can make individual units more lethal if they are equipped to take advantage of it'.[243] In this case, we are talking about making individual *navies* more lethal if they are equipped with C4ISR suites that allow and enable robust networking.

Lest anyone think this challenge is already solved in 2014 (or will solve itself shortly) the ability of navies to effectively network remains a 'wicked problem' among navies attempting to work together to deal with even basic challenges such as combating piracy - let alone dealing with more 'high-end' challenges such as AAW, ASW or ASuW. In their Newport Paper, Piracy and Maritime Crime: Historical and Modern Case Studies, Bruce Elleman, Andrew Forbes, and David Rosenberg wrote about the importance of effective maritime surveillance to counter piracy this way; 'Clearly, maritime surveillance is the key to gaining a better understanding of what is happening on the oceans, but currently, systems are not integrated within each country, let alone at regional or global levels'.[244]

In our final chapter, Chapter Six, we will suggest ways to harmonise national and naval efforts to achieve the ultimate goal - enabling near-seamless interoperability between and among navies seeking to enforce the rule of law on the global commons. It is a journey as well as a destination.

6. The Road Ahead

The previous chapters have followed parallel paths in dealing with the history and current state of coalition naval operations and the means for networking these forces for adequate command and control. Having explored these topics from the ancient to the contemporary, the logical conclusion for this treatment of networking for coalition naval operations is a reflection on how the RAN, in partnership with others, should move forward in securing the capability necessary to support networked coalition operations.

The path forward in realising the vision of network-centric coalition operations as discussed herein begins with the acceptance that the need for this capability is inherent in the need for coalition naval operations as part of the usual strategic relationships between nations today. As indicated in Chapters One and Two, this need has had many historical antecedents, especially in times of declared war. Unique to the contemporary geopolitical scene is the need for these coalitions to be established on an almost *ad hoc* basis for a wide range of naval missions. A glance around the globe will reveal multinational naval forces engaged in a wide range of missions: counter-piracy patrols, humanitarian relief operations, regional training exercises, and scientific expeditions are all examples of coalition naval forces engaged worldwide in critical missions.

How can we ensure that these forces will have a networking capability capable of supporting the range of command and control activities needed to accomplish their mission? The answer involves cooperation between potential coalition partnering navies on two levels, technical and operational.

The Technical 'Way Forward'

Ensuring that coalition naval forces will have adequate networking capability will require an ongoing dialogue on the development of networking technologies, cooperative development of those capabilities, and some form of partnership between the respective government procurement efforts of those navies.

Considering the first requirement, technological exchanges, such as the TTCP as described in Chapter Five, can be made within other regional alliances such as ASEAN or on the basis of other mutual security treaties. The advantage of the TTCP model is that it provides for the mutual study of difficult technical issues, such as AG-1/AG-6 efforts did to examine networking issues among the naval forces of the AUSCANNZUKUS nations. Leveraging the technical capabilities inherent in each nation, a TTCP-like framework allows agencies like Australia's DSTO to collaborate with similar research and development agencies in partnering coalition countries, such as DSTL in the UK, and ONR and DARPA in the US. Academia

with strong international programs can also participate in these exchanges, for example the University of Wollongong in Australia.

A step beyond the exchange of technical information under the TTCP model is the model of joint development. A prime example of this is the F-35, built primarily by the United States, but with a version that will be flown by the navies and air forces of several nations, Australia amongst them.[245] A significant bilateral example has been Australia's co-development partnership with the US Navy in the evolution of the Mk48 heavy weight torpedo. However, to date, there has been little in the way of joint development in networking systems amongst potential coalition partners, although common allies share communications resources on a regular basis. These efforts could be used as a starting point for the development of joint networking systems.

A final technical approach to ensuring that coalition naval forces have compatible networking capabilities lies in the respective procurement polices nations follow in purchasing their networking technology. The funding policies of each nation will be unique and dependent on a variety of political and economic factors and, in general, smaller nations with lean defence budgets may make short-term buys of readily available equipment and may not update this equipment frequently over time. However, the expansion of those navies that might be seen as likely coalition partners in the future provides an opportunity to standardise networking capabilities across a range of emerging national fleets. For example, India, Canada, and Russia, all recent coalition partners in counter-piracy operations in the Indian Ocean, are embarking on programs to build or procure new state-of-the-art naval forces. Hence the timing may be right for the establishment of multilateral procurement initiatives that will ensure modern networking capabilities between naval forces. In terms of a process for such an initiative, the US Navy's Foreign Military Sales (FMS) program offers an already-working model. Under it, SPAWAR conducted US $3 billion worth of FMS in command, control, and communications systems with over 40 nations in 2013.[246]

The Operational 'Way Forward'

Complementing necessary technical developments in networking capability for coalition naval operations is the need for navies to refine their operational skills in network centric operations as part of coalition forces. The opportunities for such are increasingly frequent: maritime security operations and counter-piracy operations in the Indian Ocean, humanitarian relief operations such as those undertaken in Indonesia and Haiti, and numerous multinational exercises have drawn many navies together into coalition task forces, often on short notice and with limited planning. There is a clear need to prepare fleet forces to operate together using increasingly sophisticated networking technology.

An essential component to successful network operations for coalition naval forces is adequate training beforehand. This training needs to leverage underway exercises as well as simulations, wargames, and staff training exercises to ensure that both leadership and technicians receive adequate practice in the use of afloat networks. Australia regularly participates in a wide range of exercises within the Pacific region and in other areas where national strategic interests require the Australian fleet to operate. A premier example of the ADF commitment to this type of training is the TALISMAN SABRE exercise series, conducted with the United States, to test the full range of ADF capabilities as well as its ability to take part in multi-national operations. Significantly, TALISMAN SABRE, which has a large coalition maritime scenario, also includes a technical evaluation and experimentation phase, where new networking technologies are tested by participating forces for their ability to support new coalition command processes.

Beyond TALISMAN SABRE, the model of technical experimentation in conjunction with operational training and exercises is particularly appropriate in the case of network operations. The nature of rapidly evolving information technologies demands that they be assessed *in situ,* with users and scientists working together to explore and validate their utility in an operational environment. Current development of network related applications for naval forces is based on the adoption of commercial applications. Sorting out which of these are most suited to naval operations must be done at sea, with the support of the operating forces. The United States TRIDENT WARRIOR experimentation program typifies the kind of effort needed to garner this support. During annual TRIDENT WARRIOR exercises, over one hundred new networking applications are experimented with by a dedicated task force, with rigorous analysis of the performance of each of the applications. The RAN has been a regular participant in TRIDENT WARRIOR.

The notion of training and experimenting with networking technologies at sea cannot be confined to dedicated exercises. Ongoing operations must be leveraged as training opportunities for commanders and their staffs in the use of networking technology and as part of the overall evolution of coalition command and control processes. This is particularly evident in the coalition operations being undertaken by naval forces in the Persian Gulf and Indian Ocean areas. The three combined task forces operating in this large, important, and unstable area are visible signs of the importance of naval coalitions in the modern world.[247] Command of these forces is rotated between the participating nations and the forces assigned to each vary in capabilities as assignments change. This variance requires that command personnel adapt to the networking environment as it changes and that the forces on scene work together to ensure that their collective capability to conduct networking operations is optimised. For example, the United States has developed CENTRIXS portable installations that can be temporarily installed

on smaller ships to upgrade their access to IP network services during coalition operations.[248]

Consistent with the motto of the Combined Maritime Forces operating in the Arabian Gulf and Indian Ocean areas, 'Ready Together', Australian naval forces will be called upon to act in conjunction with those of other nations for the foreseeable future. These operations are becoming increasing complex and diverse; they transcend the traditional treaty obligations that have in the past bound Australian forces to conventional warfighting operations. As the requirement to jointly support this expanding realm of operations demands the RAN look to new tactics and capabilities; there must also be the need to examine and enhance long-term partner capability to communicate, share, and collaborate with the naval forces of other nations. The model of network-centric operations is the clear foundation for this interaction. Successfully developing the capability to adhere to this model will require the combined efforts of our scientists, engineers, and operational commanders.

APPENDIX

TABLE: NETWORKING CAPABILITIES AND C2 ACTIVITIES

Networking Capabilities	C2 Activities											
	Tactical Coordination				Force Level Planning and Coordination				National Command and Control			
	Data Type	Task Supported	Advantages	Limitations	Data Type	Task Supported	Advantages	Limitations	Data Type	Task Supported	Advantages	Limitations
Voice Communications*	Voice	Tactical instructions	• Speed • Direct contact between decision makers	• Must usually be transcribed for passing to all control stations • Often in code. Must be interpreted for complete understanding	Voice	Mission planning	• Direct connection between decision makers	• Precise planning will require detailed text documents • Precise planning will require detailed diagrams, pictures	Voice	Coordination with national leadership, higher headquarters	• Speed • Direct connection between national leadership and Coalition force commander	• Difficult over long distances • Security • Detailed discussion and instructions requires text
	Voice	Weapons engagement	• Speed	• Must usually be transcribed for passing to all control stations • Often in code. Must be interpreted for complete understanding • Fire control data must be manually transcribed and entered into systems	Voice	Resolving conflicts	• Direct connection between decision makers	• Language barriers • Potential for misinterpretation	Voice	Issuing instructions to deployed force	• Speed	• Security • Potential for misinterpretation • Detailed discussion and instructions requires text
Written (Record) Communications	Text Message	Tactical instructions	• Detailed guidance easily given • Permanent record • Easily distributed to key stations	• Slow • Complex instructions must be written out and interpreted by recipient; no graphics • Impractical for execution; need to be supplemented by voice	Text Message	Resolving conflicts	• Permanent record • Clarity • Detailed	• Slow • No interactive dialogue between decision makers	Text Message	Issuing instructions to deployed force	• Secure • Detailed guidance easily given • Permanent record	• Slow • Limited interaction and dialogue

Written (Record) Communications (continued)	TADIL, Link 11/16/22, CEC	Weapons engagement	• Instantaneous orders • Direct input of data to unit fire control system	• Oversight and intervention by decision maker requires training, practice • Systems must be compatible to avoid "air gaps"	Text Message	Mission planning	• Detailed guidance easily given • Permanent record • Easily distributed to key decision makers	• Slow • Complex instructions must be written out and interpreted by recipient; no graphics • Iterative planning and interaction slow and limited	Text Message	Coordination with national leadership, higher headquarters	• Secure • Detailed guidance easily given • Permanent record	• Slow • Iterative planning and interaction slow and limited
Data Links	System Text Messages	Weapons engagement	• Instantaneous messages between units	• Distribution limited to system operators • Limited capability	TADIL, Link 11/16/22, CEC	Mission planning	• Geospatial display for easy understanding of force disposition • Automated functionality that accounts for weapons capabilities • Instantaneous transmission throughout network	• Limited opportunity to discuss options • Data possibility dated, false information in system • Limited to units with compatible systems	GCCS, related applications	Coordination with national leadership, higher headquarters	• Rapid commutations over large distances • Access to many supporting commands • Appropriate visual displays – geospatial, graphic, etc	• Limited number of units have access
	System Text Messages	Weapons engagement	• Instantaneous messages between units	• Distribution limited to system operators	System Text Messages	Mission planning	• Adjunct to other displays • Instantaneous transmission throughout network	• Limited to units with compatible systems • Distribution limited to system operators • Limited capability	System Text Messages	Coordination with national leadership, higher headquarters	• Adjunct to other displays • Instantaneous transmission throughout network	• Limited to units with compatible systems • Distribution limited to system operators • Limited capability
	Text Chat	Tactical instructions	• Near real time communications between units	• Limited capability • Users not usually at ship control stations • Priority of messages difficult to observe in most chat streams	System Text Messages	Resolving conflicts	• Instantaneous transmission throughout network	• Limited to units with compatible systems • Distribution limited to system operators • Limited capability	System Text Messages	Issuing instructions to deployed force	• Instantaneous transmission throughout network	• Limited to units with compatible systems • Distribution limited to system operators • Limited capability

IP Services	Text Chat	Weapons engagement	Near real time communications between units	• Users not usually at ship control stations • Fire control data must be manually transcribed and entered into systems	Text Chat	Mission planning	• Interaction between planners • Record of exchanges • Near real time	• Complex instructions must be written out and interpreted by recipient; no graphics • Difficult to get actual decision makers on chat stream	Text Chat	Coordination with national leadership, higher headquarters	• Interactive interaction between planners • Record of exchanges • Near real time	• Complex instructions must be written out and interpreted by recipient; no graphics • Difficult to get actual decision makers on chat stream
	Text Chat	Weapons engagement	• Near real time communications between units	• Users not usually at ship control stations	Text Chat	Resolving conflicts	• Interaction between decision makers, action officers • Record of exchanges • Near real time	• Difficult to get actual decision makers on chat stream • Not conducive to detailed discussion	Text Chat	Issuing instructions to deployed force	• Instantaneous transmission between deployed force and national headquarters	• Complex instructions must be written out and interpreted by recipient; no graphics • Difficult to get actual decision makers on chat stream
	Video (VOIP)	Tactical instructions	• Near real time communications between units • Can use full range of human communication – gestures, voice modulation	• Fire control data must be manually transcribed and entered into systems • Users not usually at ship control stations • Requires full attention • Can distract decision makers in tense situations	Video	Mission planning	• Opportunity for planners to meet "face-to-face" while discussing sensitive or complicated issues • Commanders can address each other and subordinates directly • Can use full range of human communication – gestures, voice modulation	• Bandwidth intensive • Special applications/ technology needed • Potential language barrier	Video	Coordination with national leadership, higher headquarters	• Near real time interaction between force commanders, national leadership • Opportunity for decision makers – in force and at national level – to meet "face-to-face" while discussing sensitive or complicated issues • National leaders can address deployed force commanders directly • Can use full range of human communication – gestures, voice modulation	• Bandwidth intensive • Special applications/ technology needed

IP Services (continued)	Video (VOIP)	Tactical instructions	• Near real time communications between units	• Users not usually at ship control stations	Video	Resolving conflicts	• Opportunity for planners to meet "face-to-face" while discussing sensitive or complicated issues • Commanders can address each other and subordinates directly • Can use full range of human communication – gestures, voice modulation	• Bandwidth intensive • Special applications/ technology needed • Potential language barrier	Video	Issuing instructions to deployed force	• Instantaneous transmission between deployed force and national headquarters	• Complex instructions must be written out and interpreted by recipient; no graphics • Permanent record restricted to recording
	Email	Tactical instructions	• Can use full range of human communication – gestures, voice modulation • Faster transmission than record traffic • Can be addressed to cognisant personnel • Can include diagrams, graphics as attachment	• Requires full attention • Can distract decision makers in tense situations • Not fast enough for time critical instructions • Not easily monitored at ship controls stations • Requires addressees to manually access account – potential distraction • Email structure must be developed for the force, including established protocols, servers • Special applications/ technology needed • Potential language barrier	Email	Mission planning	• Faster transmission than record traffic • Can be addressed to cognisant personnel • Can include diagrams, graphics as attachment • Allows relatively efficient dialogue between action officers, decision makers	• Email structure must be developed for the force, including established protocols, servers • Special applications/ technology needed • Potential language barrier	Email	Coordination with national leadership, higher headquarters	• Faster transmission than record traffic • Can be addressed to cognisant personnel • Can include diagrams, graphics as attachment • Allows relatively efficient dialogue between action officers, decision makers	• Email structure must be developed for the force, including established protocols, servers • Special applications/ technology needed • Specific polices regarding formality of communications
IP Services (continued)	Email	Tactical instructions	• Faster transmission than record traffic • Can be addressed to cognisant personnel • Can include diagrams, graphics as attachment	• Not fast enough for time critical instructions • Not easily monitored at ship controls stations • Requires addressees to manually access account – potential distraction • Email structure must be developed for the force, including established protocols, servers • Special applications/ technology needed • Potential language barrier	Email	Resolving conflicts	• Direct written communication between decision maker, action officers • Can include diagrams, graphics, other supplemental materials	• Email structure must be developed for the force, including established protocols, servers • Not fast enough for time critical dialogue • Special applications/ technology needed • Potential language barrier	Email	Issuing instructions to deployed force	• Direct communication between national leadership and deployed force	• Not fast enough for time critical instructions • Email structure must be developed for the force, including established protocols, servers • Special applications/ technology needed • Specific polices regarding formality of communications

*Includes visual signalling, which is still used extensively by naval forces during certain tactical evolutions. From a networking perspective, visual signalling can be thought of as very low bandwidth and slow means of exchanging text data.

NOTES

1 Royal Australian Navy, *Australian Maritime Doctrine:*, Sea Power Centre - Australia, Canberra, 2010, p. 42.

2 Royal Australian Navy, *Australian Maritime Doctrine*, pp. 40-41.

3 Naval coalitions are the primary focus of this publication and the authors make the following distinction between the terms 'coalition' and 'alliance': a coalition is characterised by the ad hoc nature of its formation while an alliance is formed as a result of formal agreements. This distinction follows the definition of 'alliance' and 'coalition' as stated in the US Department of Defense Joint Publication 1-02 (JP 1-02), DoD *Dictionary of Military and Associated Terms*. JP 1-02 defines alliances as: 'The relationship that results from a formal agreement between two or more nations for broad, long-term objectives that further the common interests of the members'. Coalitions are defined in the JP 1-02 as '[a]n arrangement between two or more nations for common action'. US Joint Chiefs of Staff Joint Doctrine Division, *Department of Defense Dictionary of Military and Associated Terms*, Washington, DC, Joint Publication 1-02, 06 November 2010, as amended through 15 December 2012, <http://www.dtic.mil/doctrine/dod_dictionary/index.html> (02 March 2013).

4 As quoted in AM Fidrych, 'Coalition Interoperability: The Long Pole in the Tent', Joint Military Operations Department, Naval War College, Newport, RI, 2000, <http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA378411> (12 September 2010).

5 PT Mitchell, *Network Centric Warfare: Coalition Operations in the age of US Military Primacy*, The International Institute for Strategic Studies, London, 2006, p. 48.

6 Thucydides, *History of the Peloponnesian War*, transcribed by R Crawley, Barns & Noble Books, New York, 2006 and VD Hanson, *A War Like No Other: How the Athenians and Spartans Fought the Peloponnesian War*, Random House, New York, 2005.

7 TG Otte, 'Dash to Peking: The International Naval Coalition during the Boxer Uprising in 1900', in BA Elleman and SCM Paine (eds), *Naval Coalition Warfare: From the Napoleonic War to Operation Iraqi Freedom*, Routledge, New York, 2008, p. 87.

8 Otte, 'Dash to Peking', *Naval Coalition Warfare*, p. 88.

9 Otte, 'Dash to Peking', *Naval Coalition Warfare*, p. 93.

10 TD Saxon, 'Anglo-Japanese Naval Cooperation, 1941-1981', *Naval War College Review,* Winter 2000, p. 65.

11 Saxon, 'Anglo-Japanese Naval Cooperation', p. 66.

12 Saxon, 'Anglo-Japanese Naval Cooperation', p. 68. See also N Sajima and K Tachikawa, *Japanese Sea Power: A Maritime Nation's Struggle for Identity*, Sea Power Centre – Australia, Canberra, 2009, p. 38.

13 Saxon, 'Anglo-Japanese Naval Cooperation', p. 68.

14 Sajima & Tachikawa, *Japanese Sea Power*, p. 140.

15 P Halpern, 'The Naval Coalition Against the Central Powers, 1914-1918', in Elleman & Pain, *Naval Coalition Warfare: From the Napoleonic War to Operation Iraqi Freedom*, Routledge, pp. 100-103.

16 Halpern, 'The Naval Coalition', p. 103.

17 JD Hornfischer, *Ship of Ghosts*, Bantam Book, New York, 2006, p. 34.

18 ICB Dear and MRD Foot, 'ABDA Command', *The Oxford Companion to World War II*, 2001. Encyclopedia.com. <http://www.encyclopedia.com/doc/1O129-ABDACommand.html> (23 May 2010).

19 Hornfischer, *Ship of Ghosts*, p. 34.

20 BA Lee, 'The Cold War as a Coalition Struggle', in Elleman & Paine, *Naval Coalition Warfare: From the Napoleonic War to Operation Iraqi Freedom*, p. 146.

21 Lee, 'The Cold War', p. 156.

22 JA Field, Jr, 'History of the United States Naval Operations: Korea', Department of the Navy - Naval Historical Center, <http://www.history.navy.mil/books/field/ch3c.htm> (02 October 2010).

23 EJ Marolda, 'The Cold War's First Conflict', US Naval Institute, <http://www.usni.org/magazines/navalhistory/2010-06/cold-wars-first-conflict > (2 October 2010).

24 M Wynd, 'From Participation to Protest: The Royal New Zealand Navy and Nuclear Testing 1957-1995', in K Young and R Mitchell (eds), *The Commonwealth Navies: 100 Years of Cooperation*, 2009 King-Hall Naval History Conference Proceedings, Sea Power Centre - Australia, 2012, pp. 129-165.

25 Marolda, 'The Cold War's First Conflict'.

26 Marolda, 'The Cold War's First Conflict'.

27 Lee, 'The Cold War', p. 147.

28 Lee, 'The Cold War', p.156.

29 JJ Sokolsky, 'Projecting Stability: NATO and Multilateral Naval Cooperation in the Post Cold War Era', North Atlantic Treaty Organization, <http://www.nato.int/acad/fellow/95-97/sokolsky.pdf> (10 October 2010).

30 M Boot, *War Made New: Technology, Warfare, and the Course of History 1500 to Today*, Gotham Books, New York, 2006, pp. 318-351. See also B Berkowitz, *The New Face of War: How War Will be Fought in the 21st Century*, The Free Press, New York, 2003 for a revealing look at the evolution of 'information-based warfare' and the challenges of networking with other militaries.

31 See Boot, *War Made New*, pp. 318-351.

32 D Taylor, 'Greenert: 1,000-Ship Navy Concept 'Alive and Well' With Shift to Pacific', InsideDefense.com, 27 September 2012, <http://insidedefense.com/201209272411399/Inside-Defense-Daily-News/DefenseAlert/greenert-1000-ship-navy-concept-alive-and-well-with-shift-to-pacific/menu-id-61.html>.

33 As of 2012, the US Maritime Strategy is being reviewed and revised to meet the current security environment and the defense priorities set forth in the 2011 Defense Strategic Guidance. See *A Cooperative Strategy for 21st Century Seapower*, October, 2007 <http://www.navy.mil/maritime/Maritimestrategy.pdf>, p. 4.

34 Department of Defense, *Sustaining US Global Leadership: Priorities for 21st Century Defense*, <http://www.defense.gov/news/Defense_Strategic_Guidance.pdf>, p. 3.

35 G Till, 'Future Navy: Competing trends in Development - Implications for Australia?' in Andrew Forbes (ed), *Australia and its Maritime Interests: At Home and in the Region*, Sea Power Centre - Australia, Canberra, 2008, p. 32.

36 G Till, 'Great Britain Gambles with the Royal Navy', *Naval War College Review*, Winter 2010, pp. 33-60. See also SJ Tangredi, 'Globalization and Sea Power: Overview and Context', in SJ Tangredi (ed), *Globalization and Maritime Power*, National Defense University, Washington, DC, 2002, pp. 1-21.

37 Robert M Gates, Eisenhower Library (Defense Spending): Remarks as Delivered by Secretary of Defense Robert M. Gates (speech, Eisenhower Library, Abilene, Kansas, 8 May 2010), <http://www.defense.gov/Speeches/Speech.aspx?SpeechID=1467> (02 March 2013).

38 Leon E Panetta, Dean Acheson Lecture: Building Partnership in the 21st Century (lecture, US Institute of Peace, Washington, DC, 28 June 2012), <http://www.defense.gov/speeches/speech.aspx?speechid=1691>.

39 Matt Siegel, 'As Part of Pact, US Marines Arrive in Australia, in China's Strategic Backyard', *The New York Times*, 04 April 2012.

40 Robert K Ackerman, 'Pacific Command Adjusts to New Regional Emphasis', *SIGNAL*, November 2012, p. 19.

41 Defense Strategic Guidance, p. 2.

42 Rita Boland, 'Information Priorities in the Asia-Pacific', *SIGNAL*, November 2012, p. 26.

43 Boland, 'Information Priorities', p. 24.

44 Boland, 'Information Priorities', p. 25.

45 Admiral Jonathan Greenert, 'Sea Change: The Navy Pivots to Asia', *Foreign Policy*, 14 November 2012, <http://www.foreignpolicy.com/articles/2012/11/14/sea_change>.

46 Greenert, 'Sea Change'.

47 C Rahman, *The Global Maritime Partnership Initiative: Implications for the Royal Australian Navy*, Papers in Australian Maritime Affairs No. 24, Sea Power Centre – Australia, Canberra, 2008. Rahman cites an article in the 20 November 2006 issue of *The Australian* as the first formal announcement of the RAN joining the Global Maritime Partnership, though; in point of fact, Australia had a rich history of participating in such activities regionally and globally.

48 Russ Shalders, 'The Royal Australian Navy: The Recent Past and the Near Future', *RUSI Defense Systems*, Spring, 2007, <http://www.rusi.org/downloads/assets/Shalders.pdf> (12 July 2010).

49 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Canberra, 2009, <www.defence.gov.au>. Executive Summary, pages 12-13. This Defence White Paper, the first such document issued in almost a decade, represents the highest level document describing the way ahead for the Australian Defence Force.

50 J Faulkner, speech made at the opening of Pacific 2010 Maritime Congress and International Maritime Exposition, Darling Harbour, Sydney, 2010, <http://www.senatorjohnfaulkner.com.au/file.php?file=/speechesindex/archive> (28 August 2014).

51 Department of Defence, *2013 Defence White Paper*, Canberra, 2013, p. 10.

52 Admiral Sir Jonathon Band, RUSI Future Maritime Operations Conference, 22-23 November 2006, London.

53 Ministry of Defence, *Defending Singapore in the 21st Century*, Singapore, 2000, <http://www.mindef.gov.sg/ds21/DS21.pdf> (07 May 2010), p. 17.

54 Ng Eng Hen, Speech by Dr. Ng Eng Hen, Minister for Defense, at 11th Shangri-La Dialogue (speech, Shangri-La Hotel, Singapore, 03 June 2012), <http://www.mindef.gov.sg/imindef/press_room/official_releases/sp/2012/03jun12_speech.html>.

55 Ministry of Defense, *Defense of Japan 2012*, Tokyo, 2012, p. 108, <http://www.mod.go.jp/e/publ/w_paper/pdf/2012/17_Part2_Chapter1_Sec1.pdf>.

56 Till, 'Great Britain Gambles with the Royal Navy', p. 44.

57 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, p. 47; see also *2013 Defence White Paper*, p. 41.

58 Sea Power Centre - Australia, 'RAN International Engagement', *Semaphore*, Issue 04, Canberra, 2008.

59 C Rahman, *Naval Cooperation and Coalition Building in Southeast Asia and the Southwest Pacific: Status and Prospect*, Working Paper No. 7, Sea Power Centre – Australia, Canberra, 2001.

60 Elleman & Paine, 'Conclusions', in Elleman & Paine, *Naval Coalition Warfare: From the Napoleonic War to Operation Iraqi Freedom*, p. 219.

61 US Navy Office of Information (CHINFO), 'Pacific Partnership 2010', *RhumbLines*, 9 July 2010.

62 CHINFO, 'Pacific Partnership 2010'.

63 US Navy Office of Information (CHINFO), 'Combined Maritime Forces', *RhumbLines*, 28 June 2010.

64 See also G Galdorisi and S Hszieh, 'Gaining the Maritime Edge: Effective Maritime Domain Awareness for the Global Maritime Partnership,' paper prepared for *RUSI Defense Systems*, Space and Naval Warfare Systems Center Pacific, 2010.

65 D Stevens, *Strength through Diversity: The Combined Naval Role in Operation Stabilise*, Working Paper No. 20, Sea Power Centre – Australia, Canberra, 2007.

66 Stevens, *Strength through Diversity*, p. 3.

67 Quoted in Stevens, *Strength Through Diversity*, p. 36.

68 Stevens, *Strength through Diversity*, p. 37.

69 Royal Australian Navy, *Australian Maritime Doctrine*, Canberra, 2010.

70 Halpren, 'Naval Coalitions Against the Central Powers', in Elleman & Paine (eds) *Naval Coalition Warfare: From the Napoleonic War to Operation Iraqi Freedom*, Routledge, New York, 2008, p. 104.

71 J Goldrick, 'The Maritime Element in the 1990-91 Gulf Crisis', in Elleman & Paine *Naval Coalition Warfare: From the Napoleonic War to Operation Iraqi Freedom*, p. 159.

72 Goldrick, 'The Maritime Element in the 1990-91 Gulf Crisis', p. 165.

73 Goldrick, 'The Maritime Element in the 1990-91 Gulf Crisis', p. 160.

74 Goldrick, 'The Maritime Element in the 1990-91 Gulf Crisis', p. 160.

75 Russ Shalders, RAN, Chief of Navy, remarks at the 10th Western Pacific Naval Symposium, 29 October - 2 November 2006, Honolulu, Hawaii.

76 G Khurana, Institute for Defence Studies and Analyses (IDSA), *Defence News*, 6 January 2007. See also, D Berlin, 'India and the Indian Ocean', *Naval War College*

Review, Spring 2006, pp. 58-89 for a more expansive treatment regarding India's maritime interests.

77 B Elleman, *Waves of Hope: The US Navy's Response to the Tsunami in Northern Indonesia*, Newport Paper 28, Naval War College Press, Newport, Rhode Island, 2007.

78 *Webster's Ninth New Collegiate Dictionary*, 9th ed., s.v. 'communication'.

79 Naval force, here, refers to communications within a single navy while a maritime coalition refers to communications between ships of many nations working together.

80 Duke of Wellington, cited in Louis J Jennings (ed), *The Correspondence and Diaries of the Late Right Honourable John Wilson Croker*, Secretary to the Admiralty from 1809 to 1830, John Murray, Albemarle Street, London, 1885, p. 276.

81 LS Howeth, *History of Communications-Electronics in the United States Navy*, Bureau of Ships and Office of Naval History, Washington, DC, 1963, p. 3.

82 HP Willmott, *Sea Warfare: Weapons, Tactics and Strategy*, Antony Bird Publication, Strettington, England, 1981, p. 17.

83 Willmott, *Sea Warfare*, p. 18.

84 Willmott, *Sea Warfare*, p. 18.

85 Howeth, *History of Communications-Electronics in the United States Navy*, p. 4.

86 Signal flags of the time of the Age of Sail were composed of different colours and geometric designs along with numeric characters that conformed to a standard set of words or instructions that were provided to ship commanders in book form – for example publications like the *Sailing and Fighting Instructions* for His Majesty's Fleet were issued to the fleet of the Royal Navy to inform commanders ships were to be controlled and arranged in battle. For further reading of signals, fighting instructions and naval tactics in the Age of Sail see WP Hughes, *Fleet Tactics: Theory and Practice*, Naval Institute Press, Annapolis, 1986 and MA Palmer, *Command at Sea: Naval Command and Control Since the Sixteenth Century*, Harvard University Press, Cambridge, 2005.

87 B Tunstall, *Naval Warfare in the Age of Sail: The Evolution of Fighting Tactics 1650-1815*, Conway Maritime Press Limited, London, 1990, pp. 8-9.

88 Tunstall, *Naval Warfare in the Age of Sail*, p. 80.

89 R Adkins, 'Trafalgar: A Signal Victory', *Geographical 77*, no. 10, 2005, p. 59.

90 Tunstall, *Naval Warfare in the Age of Sail*, p. 80.

91 Tunstall, *Naval Warfare in the Age of Sail*, pp. 8 and 252.

92 Adkins, 'Trafalgar: A Signal Victory', p. 59.

93 Adkins, 'Trafalgar: A Signal Victory', p. 59.

94 EB Potter, *Sea Power: A Naval History*, (2nd ed), Naval Institute Press, Annapolis, 1981, p. 78.

95 Willmott, *Sea Warfare*, p. 27 and also Potter, *Sea Power*, p. 109.

96 John Perryman, 'Visual Signalling in the Royal Australian Navy', *Semaphore*, Issue 8, Sea Power Centre - Australia, Canberra, 2006.

97 A Hezlet, *Electronics and Sea Power*, Stein and Day, New York, 1975, p. 3.

98 NAM Rodger, author's personal notes taken at the Royal Australian Navy King-Hall Naval History Conference, Sydney/Canberra, Australia , 24 and 26-27 July 2007.

99 Howeth wrote of the US Navy's experience with the electric telegraph: By 1890 commercial telegraphic or cable facilities were available in practically every port frequented by the Navy. These facilities provided rapid communication between the Navy Department and the commanders of squadrons, when in port. This permitted the Navy Department to keep its commanders advised of the political situation, but lessened the amount of discretion allowed them. (Howeth, *History of Communications-Electronics*, pp. 10-11).

100 N Friedman, 'Netting and Navies: Achieving a Balance', in Andrew Forbes (ed), *Sea Power: Challenges Old and New*, Halstead Press, Sydney, 2007, pp. 177-200.

101 Friedman, 'Netting and Navies'.

102 Letter by E Whitman, Assistant Secretary of the Navy for Research, Development, and Acquisition, to a young man in Oklahoma explaining the history of naval communications, 1992. A copy of the letter is held by the authors.

103 Letter by Whitman, 1992. See also M Witt, 'Of Signal Significance', *Asian Defence Journal*, December 1997, pp. 34-40.

104 Great care was taken to ensure the health and well being of these important birds. In 1918, the Office of Naval Operations published the I*nstructions on Reception, Care and Training of Homing Pigeons in Newly Installed Lofts at US Navy Air Bases* to spell out the proper care and feeding of all Navy homing pigeons. An electronic version of the document can be found at the Navy Department's library website: <http://www.history.navy.mil/library/special/homing_pigeons.htm>.

105 Letter by Whitman.

106 Friedman, 'Netting and Navies'.

107 Letter by Whitman.

108 Letter by Whitman. See also Witt, 'Of Signal Significance'.

109 EA Smith, Jr, 'Network-Centric Warfare: What's the Point', *Naval War College Review*, Winter, 2001, pp. 65-66. See also DW Isom, 'The Battle of Midway: Why the Japanese Lost', *Naval War College Review*, Summer, 2000, pp. 60-63.

110 Potter, *Sea Power*, pp. 296-301.

111 RB Frank, *Guadalcanal: The Definitive Account of the Landmark Battle*, Penguin Books, New York, 1990, pp. 444 and 460.

112 NAM Rodger, 'Communications in Naval Warfare', in David Stevens (ed), *Naval Networks: The Dominance of Communications in Maritime Operations*, Sea Power Centre - Australia, Canberra, 2012, pp. 7-20.

113 N Friedman, 'Wide Open Space: Navies Exploit Satellite Revolution', *Jane's Navy International*, vol. 105, no. 3, 2000. Radio relay ships were classified as AGMR and were known as Major Communications Relay Ships. AGMR were converted World War II aircraft carriers that patrolled the coasts of Vietnam, providing a sea based radio relay system to allow ship to shore and ship to ship communications where land based radio stations were hard to come by. More information on AGMR can be found at the website for the USS *Annapolis* AGMR-1 <http://www.boston.quik.com/kurtdold/tonkin1.html>.

114 Letter by Whitman.

115 Hughes, *Fleet Tactics*, p. 171.

116 Hughes, *Fleet Tactics*, p. 172.

117 Hughes, *Fleet Tactics*, p. 150.

118 N Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars*, Naval Institute Press, Annapolis, Maryland, 2009, p. 65.

119 Friedman, *Network-Centric Warfare*, p. 66.

120 Friedman, *Network-Centric Warfare*, p. 70.

121 Friedman, *Network-Centric Warfare*, p.124.

122 Advanced Research Projects Agency Network (ARPANET)

123 M Boot, *War Made New: Technology, warfare, and the Course of History*, Gotham Books, New York, 2006, p. 311.

124 N Friedman, *Terrorism, Afghanistan, and America's New Way of War*, Naval Institute Press, Annapolis, 2003, p. 110.

125 See the US Naval Historical Centre's website: <http://www.history.navy.mil/branches/org9-4.htm>. The site provides a historical overview of the size of the US Navy from 1917 to the present day. See also the Naval Vessel Register at NAVSEA for the most current fleet size. The site can be found at: <http://www.nvr.navy.mil/nvrships/FLEET.HTM>.

126 FW Kagan, *Finding the Target: The Transformation of American Military Policy*, Encounter Books, New York, 2006, p. 169.

127 GR Sullivan and JM Dubik, *Land Warfare in the 21st Century*, Strategic Studies Institute, Carlisle Barracks, 1993, p. xx.

128 MC Libicki and SE Johnson, (eds), *Dominant Battlespace Knowledge*, National Defense University, Washington, DC, 1995, p. iv. See also HK Ullman and JP Wade, *Shock and Awe: Achieving Rapid Dominance*, National Defense University, Washington, DC, 1996.

129 US Department of Defense, 'Report of the Quadrennial Defense Review', Washington, DC, 1997, <http://www.dod.gov/pubs/qdr/sec7.html> (01 August 2010).

130 F Kagan, *Finding the Target: The Transformation of American Military Policy*, Encounter Books, New York, 2006, p. 254.

131 AK Cebrowski and JH Garstka, 'Network-Centric Warfare-Its Origin and Future', US Naval Institute *Proceedings*, January, 1998.

132 Cebrowski & Garstka, 'Network-Centric Warfare'.

133 Cebrowski & Garstka, 'Network-Centric Warfare'.

134 JR Blaker, *Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare*, Praeger Security International, Westport, 2007, pp. 18-19.

135 Office of the Secretary of Defense, *Network Centric Warfare: Department of Defense Reports to Congress*, Department of Defense, 2001, p. 3-1. Document can be found at <http://www.dodccrp.org/files/ncw_report/report/ncw_main.pdf>.

136 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Canberra, 2009, p. 67.

137 Royal Australian Navy, *Australian Maritime Doctrine,* p. 78

138 Royal Australian Navy, *Australian Maritime Doctrine,* p. 159.

139 Royal Australian Navy, *Australian Maritime Doctrine,* p. 146-147.

140 N Friedman, *Network-Centric Warfare*, p. ix.

141 L Thompson, *Networking the Navy: A Model for Modern Warfare*, Lexington Institute, Arlington, 2003, pp. 3-4. At the core of Copernicus were four overriding goals: to provide a common tactical picture to all members of the naval force; to comprehensively connect them in a web of instantaneous voice and data links; to compress the steps involved in moving information from sensors to shooters; and to conduct information operations that would degrade enemy warfighting capabilities.

142 A Clemins, 'IT-21: The path to information superiority,' *CHIPS*, July 1997.

143 Cebrowski & Garstka, 'Network centric warfare: its origin and future', pp. 29-35.

144 Thompson, *Networking the Navy: A Model for Modern Warfare*, p. 6.

145 See V Clark, 'Sea Power 21: projecting decisive joint capabilities,' US Naval Institute *Proceedings*, October 2002.

146 See, R Mayo and J Nathman, 'ForceNet: Turning information into power,' US Naval Institute *Proceedings*, February 2003, pp. 42-46. Also, it should be noted that the word 'Forcenet' is spelled differently in different resources in the expansive literature on the subject. Generally, in US Navy parlance, it is spelled FORCEnet. This is because, then-CNO Admiral Vern Clark wanted to emphasise that this was something that supported 'the FORCE' (meaning naval forces).

147 Thompson, *Networking the Navy: A Model for Modern Warfare*, p. 6. See also Loren Thompson, *Netting the Navy*, Lexington Institute, Arlington, 2008, pp. 1-7 for a more contemporary look at the same subject.

148 Until 2010, the US Navy Program Guide, the yearly overview of the systems, programs and initiatives the US Navy is pursuing to deliver a future navy, was organised around the four Sea Power 21 'pillars' of Sea Strike, Sea Shield, Sea Basing and FORCEnet. Grouped under FORCEnet were all the US Navy's C4ISR systems that supported network-centric warfare. And while the Navy *Program Guide 2010* (Washington, DC US Navy, 2001, <http: www.navy.mil/navydfata/policy/seapower/spne10/top-spne10.html> did not carry forward this Sea Power 21 taxonomy of grouping USN programs, the C4ISR section of the *Program Guide* featured all of the USN programs supporting network-centric warfare, from CANES (Common Afloat Network Enterprise System), to JTIDS (Joint Tactical Information Distribution System), to CENTRIXS-M (Combined Enterprise Regional Information Exchange System Maritime) to literally dozens of others.

149 Department of Defence, *Future Maritime Operating Concept – 2025: Maritime Force Projection and Control*, Canberra, 2009, pp. 15-16. This unclassified version of the *Future Maritime Operating Concept* (FMOC), co-signed by the Chief of Defence Force and Chief of Navy, represents the vision for how the RAN will operate in the year 2025 and provides a window on what technological capabilities this navy must possess.

150 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Canberra, 2009, Executive Summary, Pages 11-14. Importantly, this capstone publication has an entire sub-chapter dedicated to Information Superiority. For a detailed analysis of this capstone publication, see McCaffrie and Rahman, 'Australia's 2009 Defence White Paper: A Maritime Force for Uncertain Times,' *Naval War College Review*, Winter 2010, pp. 61-76. Importantly for this book, they note; 'The intent is for the ADF to maintain a strategic capability edge in the region, by continuing to exploit and apply advanced technologies.'

151 Canadian Defence Force, *Leadmark – The Navy's Strategy for 2020*, Directorate of Maritime Strategy, Ottawa, 2001.

152 J Kiszely, 'Achieving High Tempo: New Challenges,' *RUSI Journal*, December 1999.

153 *NATO 2020: Assured Security; Dynamic Engagement: Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO*, NATO Public Diplomacy Division, Brussels, 2010, pp. 37-40.

154 N Friedman, 'Netting and Navies', pp. 185-186

155 For an extensive – and expansive – look at this history, we have found that Norman Friedman's *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars* to be the definitive reference work.

156 Space and Naval Warfare Systems Command, *Naval IT, C4ISR, Space Systems, and Enterprise Support: Today and Tomorrow*, SPAWARSYSCOM, San Diego, 2009, p. 3, <www.spawar.navy.mil>.

157 R Kerber and V Vitto, *Report of the Defense Science Board Task Force on Department of Defense Policies and Procedures for the Acquisition of Information Technology*, Department of Defense, Washington, DC, 2009, p. iii.

158 CANES is the Consolidated Afloat Networks and Enterprise Services. NGEN is the Next Generation Enterprise Network.

159 P Mitchell, 'Small Navies and Network-centric Warfare: Is There a Role?' *Naval War College Review*, Spring 2003, p. 85.

160 We picked 2030 explicitly for two reasons: it is the planning horizon that the 2009 Defence White Paper, *Defending Australia in the Asia Pacific Century: Force 2030* looks out to, and because 20 years hence is about as far out as anyone in the intelligence, military, technology, industry or academic communities is comfortable making predictions.

161 AIS, the Automatic Identification System, is a short-range tracking system used by ships and by Vessel Traffic Services (VTS) for identifying and locating vessels by electronically exchanging data with other nearby ships and VTS stations.

162 Take, for example, the MQ-1 Predator system, whose role supporting operations in Iraq and Afghanistan has been recounted numerous times both within the DoD and in the press. Their ability as a force multiplier usually goes unquestioned, until one considers the footprint that accompanies the system. The USAF fact sheet on the MQ-1 notes that the typical 'fully operational system consists of four aircraft (with sensors), a ground control station, a Predator Primary Satellite Link, or PPSL, along with operations and maintenance crews for deployed 24-hour operations.' For those four aircraft, this all involves 55 or more personnel, who rotate regularly after a few months in most cases. While a superb platform, the idea that we can afford to man all the unmanned systems we need is tenuous, at best.

163 See, for example, M Fetsch, C Mailey, and S Wallace, 'UV Sentry', paper presented at the *Association for Unmanned Vehicle Systems International, 34th Annual Symposium and Exhibition*, Washington, DC, 6-9 August, 2007; R Kilgore et al, 'Mission Planning and Monitoring for Heterogeneous Unmanned Vehicle Teams: A Human Centered Perspective,' paper presented at the *American Institute of Aeronautics and Astronautics Conference*, Rohnert, 7-10 May, 2007; CE Nehme et al, 'Generating Requirements for Futuristic Heterogeneous Unmanned Systems,' *Proceedings of the 50th Annual Meeting of the Human Factors and Ergonomics Society*, San Francisco, 2006; and PW Singer, *Wired for War? Robots and Military Doctrine*, Penguin Press, New York, 2009.

164 The Air Force Research Laboratory's Information Directorate is working with Space and Naval Warfare Systems Command to develop these publish-subscribe-query-broker technologies.

165 This hacking was widely reported in the international media. For a well-nuanced discussion, see McCaffrie & Rahman, 'Australia's 2009 Defence White Paper: A Maritime Force for Uncertain Times,' p. 66 for additional details on China's hacking, and especially that targeted against Australian entities as well as Australia's efforts to thwart such attacks.

166 McCaffrie & Rahman, 'Australia's 2009 Defence White Paper: A Maritime Force for Uncertain Times,' pp. 73-74.

167 Mitchell, 'Small Navies and Network-centric Warfare: Is There a Role?', p. 84.

168 J Mattis remarks at the Joint Warfighting Symposium, 13 May 2010, <www.jfcom.mil/newslink/storyarchive/2010/pa050110.html>. In addition to his role as Commander of the US Joint Forces Command, General Mattis is also Commander Allied Force Transformation, an important NATO 'hat' that involves seeking solutions to issues of allied and coalition networking challenges.

169 Royal Australian Navy, *Australian Maritime Doctrine*, p. 106.

170 United States Navy battle formations are most often deployed as Carrier Strike Groups (CSG) or as Expeditionary Strike Groups (ESG). CSG are built around a large-deck aircraft carrier operating tactical jet aircraft, and ESG are built around a large-deck amphibious ship operating VSTOL aircraft and helicopters.

171 Mitchell, 'Small Navies and Network-Centric Warfare: Is there a Role'?, pp. 88-89.

172 P Mitchell, 'Small Navies and Network-centric Warfare: Is There a Role? Canada and US Carrier Battlegroup Deployments,' briefing presented at the 8th International Command and Control Research and Technology Symposium, Washington, DC, 17-19 June 2003. Mitchell's statement did not come from his prepared presentation, but from the question and answer period following his formal presentation.

173 Department of Defense, *Military Transformation: A Strategic Approach*, Washington, DC, 2003, pp. 1-36, accessed at: Internet <oft.osd.mil>. This publication is the capstone publication of the Office of Force Transformation, US Department of Defense.

174 CENTRIXS is US Navy Combined Enterprise Regional Information Exchange System. See B Carter and D Harlor, 'Combined Operations Wide Area Network (COWAN)/Combined Enterprise Regional Information Exchange System (CENTRIXS),' *Biennial Review*, San Diego, CA: Space and Naval Warfare Systems Center San Diego, 2003, p. 87, for a detailed technical description of CENTRIXS. See also Mitchell, 'Small Navies and Network-centric Warfare: Is There a Role?,' p. 90 for another nation's view of CWAN (COWAN) and CENTRIXS.

175 McCaffrie & Rahman, 'Australia's 2009 Defence White Paper: A Maritime Force for Uncertain Times,' pp. 71-72.

176 Mitchell, 'Small Navies and Network-Centric Warfare: Is There a Role?', p. 91.

177 See, for example, DC Gompert, RL Kugler, and MC Libicki, *Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs*, National Defense University Press, Washington, DC 1999 for one of the earliest works that explored the challenges involved in ensuring that network-centric warfare investments and technology lead to more effective networking between and among allies and coalition partners. See also

J Thomas, *The Military Challenges of Transatlantic Coalitions*, Adelphi Paper 333, IISS, London, 2000 for a European point of view on this issue.

178 For a discussion of the implications of doctrine on coalition naval forces, see JJ Tritten, 'Implications for Multinational Naval Doctrine', in Tangredi, *Globalization and Maritime Power*, pp. 259-279.

179 For example, see RK Ackerman, 'British Defence Information Technology Sees Uncertain Future', *SIGNAL*, August 2009, pp. 85-88.

180 In the future the US Navy will focus its shipboard network integration on the Consolidate Afloat Network and Enterprise Services (CANES) architecture. This system will integrate CENTRIXS with other shipboard network service aboard US Navy ships. See Sharon Anderson, 'CANES: Consolidated, Dynamic, and Combat Ready', *CHIPS*, July-September 2009, pp. 6-8.

181 For an insightful consideration of how networking technology has impacted daily life, see TL Freidman, *The World is Flat: a Brief History of the Twenty-First Century*, Farrar, Straus and Giroux, New York, 2005, pp. 159-172.

182 The C2 activities used for discussion herein are one distillation of various theories of command and control, most suited to the naval force that is the central focus of this discussion. DS Alberts and RE Hayes, in *Understanding Command and Control*, DoD CCRP, 2006, pp. 32-48, stipulate that there are seven function for C2: establishing intent; determining roles, responsibilities and relationships; establishing rules and constraints; monitoring and assessing the situation and program; inspiring, motivating, and engendering trust; training and education; and provisioning. These more general functions are accomplished within the framework of the three more specific C2 activities discussed here.

183 DS Alberts, JJ Garstka, FP Stein, *Network Centric Warfare: Leveraging Information Superiority*, DoD CCRP, 1999, pp. 97-98. Alberts and his co-authors point out the limitation of relying on voice only in managing engagement.

184 For a complete history of the Link program, including its adoption by the Australian Navy and other coalition navies, see Friedman 'The Naval Tactical Data System', *Network-Centric Warfare*, pp. 74-93.

185 Alberts et al., *Network Centric Warfare*, p.146, describes how the CEC fits into the larger concept of network centric warfare

186 According to the commander of the US Navy's SPAWAR, Michael Bachmann, USN, even large US Navy ships have access to about half the bandwidth – 0.64Mbs – as the average US residence, with small combatants having about half that. Given current commercial trends, Bachmann predicts that the standard home will have 250 times the IP bandwidth as a US guided missile destroyer by 2014, and 100 times that of a US aircraft carrier. Data came from the briefing given to the ComNexus San Diego Military Interest Group, 7 December 2006.

187 For a discussion of 'heterogeneity' as it applies to coalition information systems, see AJ Krygiel, *Behind the Wizard's Curtain*, DoD CCRP, 1999, pp.41-46

188 WP Hughes, *Fleet Tactics and Coastal Combat* (2nd ed), Naval Institute Press, Annapolis, 2000, talks about sensor employment as part of 'scouting,' and links the scouting phase of a naval battle with the time needed for the commander to receive and process the information gathered, part of his command and control phase.

189 DS Alberts, RK Huber, J Moffat, *NATO NEC C2 Maturity Model*, DoD CCRP, 2010.

190 The FORCEnet Functional Capabilities are available at < http://forcenet.navy.mil/concepts/capabilities-annex.pdf>.

191 Chew Men Leong, 'Opening Address for Ex Carat 2005 by Fleet Commander', <www.mindef.gov.sg/imindef/news_and_events/nr/2005/may/31may05_nr/31may05_speech.html.print.html?Status=1> (10 June 2010).

192 See, for example, Australian Strategic Policy Institute, *Australian Defence Almanac 2010-2011*, Canberra, 2010, especially pp. 102-108 for a comprehensive listing of ADF overseas deployments from 1947-2009 and pp. 109-110 for a listing of 2010 ADF overseas deployments. While similar information is contained in other publications ADF overseas deployments captures this in one source. A close perusal of this information makes it clear that few nations have the scope of coalition partners that Australia has and also makes it clear that these partners cover a wide spectrum from 'high end' navies, to 'middle powers' to smaller, regional navies with only rudimentary C4ISR capabilities. This makes Australia one of the key stakeholders in efforts to achieve near-seamless coalition interoperability.

193 The Technical Cooperation Program: TTCP document DOC-SEC-3-2005, *A Beginner's Guide to the Technical Cooperation Program*, 1 September 2005, <www.dtic.mil/ttcp/>. This document published on TTCPs public website, is a concise explanation of its structure and purpose, as well as a useful capture of the purpose of other five-eyes organisations. This explanation of cooperation between and among AUSCANNZUKUS nations in general and under the auspices of TTCP has been previously described by Galdorisi and Sutton in their contribution 'Coalition Interoperability: How Much is Enough and How to Quantify It', in Forbes (ed), *Sea Power: Challenges Old and New*, pp. 147-175, but has been adapted and updated for this publication.

194 TTCP, *A Beginner's Guide to the Technical Cooperation Program*, p. 4.

195 Mitchell, 'Small Navies and Network-centric Warfare: Is There a Role?' p. 84. See also, N Friedman, *World Naval Weapons Systems 1997-1998*, Naval Institute Press, Annapolis, 1997, p. 28.

196 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, p. 136.

197 TTCP, *A Beginner's Guide to the Technical Cooperation Program*.

198 TTCP, *A Beginner's Guide to the Technical Cooperation Program.*

199 Importantly, some of this qualitative work has addressed coalition operations, confirming the importance of networking in the multi-lateral operations. See, for example, D Gompert et al, *Mind the Gap: Promoting a Transatlantic Revolution in Military Affairs*, National Defence University Press, Washington, DC, 1999; J Thomas, *The Military Challenges of Transatlantic Coalitions*, Adelphi Paper 333, IISS, London, 2000; G Adams, 'Strength in Numbers: The European Allies and American Defence Planning,' in C Williams (ed), *Holding the Line: US Defence Alternatives for the Early 21st Century*, MIT Press, Cambridge, 2001; and G Adams et al, *Bridging the Gap: European C4ISR Capabilities and Transatlantic Interoperability*, Defence and Technology Paper 5, National Defence University Press, Washington, DC, 2004. These studies, and others like them, emphasise the importance of coalition operations and, by extension, coalition partners operating in a networked fashion.

200 While little quantitative work on network-centric operations has been done based on from-the-ground-up modelling and simulation, the United States Assistant Secretary of Defense for Networks and Information Integration (ASD NII), under the auspices

of the Command and Control Research Program (CCRP), has reviewed the results of both exercises and wartime events to draw some quantitative results regarding the value of networking. MAR AG-1 and AG-6 reviewed this CCRP material in evaluating 'best practices' for the conduct of their studies, and this CCRP work informed much of the group's work. See <www.dodccrp.org> to access the totality of the CCRP effort, including several books that describe these early efforts to quantify the benefits of networking.

201 Some TTCP MAR AG-1 reports, including the final *Network-Centric Maritime Warfare Study Capstone Report* (TR-MAR-12-2004) are labelled "For Official Use Only" because the document(s) 'Contain information that is provided in confidence to the TTCP Governments.' However, some of these reports do allow for unlimited distribution. Due to the focused outreach efforts by MAR AG-1, the results of the team's work were reported in open venues such as the International Command and Control Research and Technology Symposia (ICCRTS).

202 I Grivell et al., *A Review of Analytic Techniques Applicable to the Study of Network Centric Warfare*, TTCP TR-MAR-9-2003, May 2003.

203 C Davis et al., *Key Issues in Coalition Network-Centric Maritime Warfare*, TTCP TR-MAR-10-2003, January 2004.

204 See G Galdorisi and D Sutton, 'A Technical Approach to Coalition Interoperability,' paper presented at the 11th International Command and Control Research and Technology Symposium, Cambridge, United Kingdom, September 2006, <www.dodccrp.org>. See also M Hazen et al., 'The Analysis of Network-Centric Maritime Interception Operations (MIO) Using Queuing Theory,' presentation at the 8th International Command and Control Research and Technology Symposium, Washington, DC, 17-19 June 2003; R Klingbeil et al, 'Utilizing Network-Enabled Command and Control Concepts to Enhance ASW Effectiveness,' presentation at the 9th International Command and Control Research and Technology Symposium, Copenhagen, Denmark, 14-16 September 2004; and D Galligan et al., 'Net Centric Maritime Warfare – Countering a 'Swarm' of Fast Inshore Attack Craft,' presentation at the 10th International Command and Control Research and Technology Symposium, McLean, 13-16 June 2005, all accessed at <www.dodccrp.org>.

205 M Hazen et al., 'The Analysis of Network-Centric Maritime Interception Operations (MIO) Using Queuing Theory,' The majority of the detailed analysis of the TACSIT contained herein is excerpted directly from this paper as it is the primary repository of this TTCP MAR AG-1 work that is available for unlimited distribution.

206 Hazen, 'The Analysis of Network-Centric Maritime Interception Operations (MIO) Using Queuing Theory,' pp. 8-9.

207 Remarks by Admiral W Doran, Commander, United States Pacific Fleet, at the 'West 2005' Conference, San Diego, 2 February 2005.

208 Klingbeil et al, 'Utilizing Network-Enabled Command and Control Concepts to Enhance ASW Effectiveness'. The majority of the detailed analysis of the TACSIT contained herein is excerpted directly from this paper; as it is the primary repository of this TTCP MAR AG-1 work that is available for unlimited distribution.

209 For a careful examination of the definitions and concepts of SA and SSA, see AA Nofi, *Defining and Measuring Shared Situational Awareness*, CNA Research Memorandum, CRM D0002895.A1/Final, November 2000.

210 USJFCOM, Multinational Experiment III; <www.jfcom.mil/about/experiments/mne3.htm> 2003.

211 KM Sullivan and I Grivell, *QSIM: A Queuing Theory Model with Various Probability Distribution Functions*, NUWC-NPT Technical Document 11,418, 14 March 2003 (updated by I Grivell, December 2003).

212 Klingbeil, 'Utilizing Network-Enabled Command and Control Concepts to Enhance ASW Effectiveness', pp. 17-18.

213 *Department of Defense Joint Net Centric Capabilities*, Office of the Assistant Secretary of Defense for Networks and Information Integration, Washington, DC, 2003.

214 Galligan, 'Net Centric Maritime Warfare – Countering a "Swarm" of Fast Inshore Attack Craft.' The majority of the detailed analysis of the TACSIT contained herein is excerpted directly from this paper; as it is the primary repository of this TTCP MAR AG-1 work that is available for unlimited distribution.

215 M Bucchi and M Mullen, 'Sea Shield: Projecting Global Defensive Assurance,' US Naval Institute *Proceedings*, November 2002, pp. 56-59.

216 Three types of FIAC threats were modelled, and these types represented the generally accepted FIAC types described in the naval literature on the subject. Type 1 FIAC are those represented by a jet ski or boson whaler with rocket propelled grenade (RPG) weapons or a large-blast bomb used in a suicide attack. Type 2 FIAC are those represented by larger 'Boghammer' class boats with unguided multiple-launch bombardment rockets or with larger anti-tank guided weapons. Type 3 FIAC are those represented by small fast patrol boats (FPB) typified by the Super Dvora, with smaller anti-ship missiles or torpedo armament.

217 Maritime Systems Group Terms of Reference for AG-6 (internal document).

218 SPAWAR Systems Center San Diego was renamed SPAWAR Systems Center Pacific in 2008 in accordance to the 2005 Base Realignment and Closure law.

219 See V Clark, 'Sea Power 21: Projecting Decisive Joint Capabilities', and R Mayo and J Nathman, 'FORCEnet, Turning Information Into Power,' US Naval Institute *Proceedings*, February 2003, for two of the earliest articles in the open literature regarding Sea Power 21 and FORCEnet. The capitalisation of 'FORCE' while 'net' remained in small letters was done purposefully by the CNO. This was done to emphasise that FORCEnet was about providing a warfighting capability to the naval *force*, and was not about 'the net'.

220 *FORCEnet: A Functional Concept for the 21st Century*, p. 6, <www.enterprise.spawar.navy.mil/getfile.cfm?contentId=816&type=R>. See also; *FORCEnet: A Functional Concept for Command and Control in the 21st Century*, Annex, Version 20, June 2006.

221 David Alberts and Richard Hayes, *Power to the Edge: Command and Control in the Information Age*, Department of Defense Command and Control Research Program, Washington, DC, 2003.

222 The body of work produced by the US DoD Command and Control Research Program (CCRP) provides much of the theoretical, conceptual and analytical basis for network-centric operations as it is generally understood and practiced by military units. For more on the CCRP, see <www.dodccrp.org.>

223 *FORCEnet: A Functional Concept for the 21st Century*, pp. 12-19.

224 Office of the Chief Engineer, Space and Naval Warfare Command, *FORCEnet Architecture and Standards, Volume I (Operational and Systems View) and Volume II (Technical View)*, SPAWAR, San Diego, 2005.

225 *FORCEnet Architecture and Standards Volume II (Technical View)* clearly defines the objective that the technical community must achieve in designing FORCEnet: 'develop a naval networking infrastructure and integrated applications suite with full interoperability among the service components, joint task force elements, and allied/coalition partners. The FORCEnet Architecture will ensure that design decisions made by component programs are consistent with the FORCEnet blueprint and incorporate common engineering, information, protocols, computing, and interface standards across various computing environments and platforms. This blueprint will be based on joint and commercial standards, with development and implementation coordinated with transformational initiatives, the Army, Air Force, and Coast Guard, as well as Joint commands and allies'.

226 SSC San Diego scientists and engineers have briefed the Composeable FORCEnet concept to literally hundreds of military, industry, and academic professionals over the past several years. See, for example, G Galdorisi et al., 'Composeable FORCEnet Command and Control: The Key to Energizing the Global Information Grid to Enable Superior Decision Making', *Proceedings of the 2004 Command and Control Research and Technology Symposium*, June 2004, <www.dodccrp.org>.

227 D Alberts and R Hayes, *Understanding Command and Control*, DoD Command and Control Research Program, Washington, DC, 2006, p. 91. The Command and Control Research Program (CCRP) is part of the Office of the Assistant Secretary of Defense (NII) and has the mission to improve the DoD's understanding of the national security implications of the Information Age and seeks to bridge the world of the operational, technical and analytical with that of the educational community.

228 *Department of the Navy: Information Management and Information Technology Strategic Plan* (Washington, DC: Department of the Navy Chief Information Officer, 2006), <www.doncio.navy.mil/fy06stratplan/>, p. 9:

> Scientists at Space and Naval Warfare Systems Center, San Diego originated a web-centric concept demonstration titled Composeable FORCEnet that uses a publish and subscribe schema, allowing decision-makers to collate and display data from many different sources. OPNAV directed advanced installation of the concept in the 7th Fleet area of responsibility, and it is now installed at CTF-74 and on board USS Blue Ridge and USS Kitty Hawk. Composeable FORCEnet provides watchstanders and operational commanders with vastly improved and more rapid shared situational awareness, leading to a major improvement in asymmetric warfighting in the Pacific.

229 *A Functional Concept for Command and Control in the 21st Century and FORCEnet: A Functional Concept for Command and Control in the 21st Century*, Annex, Version 20, June 2006, www.enterprise.spawar.navy.mil/getfile.cfm?contentId=816&type=R. See also, V Clark, 'Sea Power 21: Projecting Decisive Joint Capabilities'; and Mayo and Nathman, 'FORCEnet, Turning Information into Power'.

230 *FORCEnet: A Functional Concept for Command and Control in the 21st Century*.

231 AG-6's efforts to select a scenario that reflected a realistic balance among multiple missions was informed by the work of the Command and Control Research Program (CCRP), especially the following publications: D Alberts and R Hayes, *Command Arrangements for Peace Operations*, CCRP Publications, Washington, DC, 1996; B Hayes and J Sands, *Doing Windows: Non-Traditional Military Responses to Complex Emergencies*, CCRP Publications, Washington, DC, 1998; K Avruch et al, *Information*

Campaigns for Peace Operations, CCRP Publications, Washington, DC, 1999; and H Binnendijk and S Johnson, *Transforming for Stabilization and Reconstruction Operations*, CCRP Publications, Washington, DC, 2004, among others.

232 For this scenario, the United States ESG would include three amphibious assault ships (built around a large-deck command ship), one cruiser, two destroyers, three littoral combat ships, and one attack submarine. Australia would contribute two *Anzac* frigates, two other frigates, and one destroyer. Canada could send up to a task group (including a destroyer, two frigates, a submarine and a replenishment ship). New Zealand would send two *Anzac* frigates, one multi-role vessel, and one replenishment ship. The United Kingdom would send one large deck amphibious ship, two smaller amphibious ships and one replenishment ship.

233 See J Clarkson, G Galdorisi, J Grossman, M Reilley and C Priebe, 'Composeable FORCEnet,' in *SSC San Diego Biennial Review 2006,* San Diego, SPAWAR Systems Center San Diego, 2006; D Alberts and R Hayes, *Understanding Command and Control*; *Department of the Navy: Information Management and Information Technology Strategic Plan*, Department of the Navy Chief Information Officer, Washington, DC, 2006; and G Galdorisi et al., 'Composeable FORCEnet Command and Control: The Key to Energizing the Global Information Grid to Enable Superior Decision Making,' *Proceedings of the 2004 Command and Control Research and Technology Symposium*, June 2004, <www.dodccrp.org>.

234 See, for example, Kim-Song Tan and Sock-Yong Phang, *From Efficiency-Driven to Innovation-Driven Economic Growth: Perspectives from Singapore*, World Bank Policy Research Working Paper No. 3569, April, 2005. Available at SSRN: <http://ssrn.com/abstract=712623>. See also M Kanellos, 'Singapore: One Nation under Wi-Fi', *c|net news.com*, 28 August 2006, < http://news.com.com/2100-1039_3-6110189.html>.

235 Singapore has attracted a number of IT companies like Hewlett Packard and Motorola who have established an R&D division to team with Singapore companies to develop new networking technologies. Hewlett Packard's Singapore R&D division is working on next-generation networking servers and Motorola has teamed with the Singapore Design Centre to work on new mobile equipment designs. See, Intelligent Nation 2015 Steering Committee, 'Innovation. Integration. Internationalisation', June 2006, <www.in2015.sg/pdf/01_iN2015_Main_Report.pdf>.

236 A Soto, 'Maritime Information Sharing Strategy: A Realistic Approach for the American Continent and the Caribbean', *Naval War College Review*, Summer 2010, pp. 139-152.

237 L Wentz, cited in A Krygiel, *Beyond the Wizard's Curtain: An Integration Environment for a Systems of Systems*, DoD CCRP, Washington, DC, 1999, p. 205.

238 McCaffrie & Rahman, 'Australia's 2009 Defense White Paper: A Maritime Force for Uncertain Times', pp. 73-74. As they point out, Australia's 2000 Defence White Paper adopted the same 'continentalist doctrine' as the 1997 strategy. See also McCaffrie and Rahman's footnote 58 in their *War College Review* article that connects the 1997 strategy to the so-called 'Dibb Report' of 1986.

239 Royal Australian Navy, *Australian Maritime Doctrine*, p. 151.

240 Royal Australian Navy, *The Navy Contribution to Australian Maritime Operations*, Sea Power Centre - Australia, 2005, p. 197.

241 A Forbes and P Leavy, 'RAN International Engagement', in G Gilbert and N Stewart (eds), *Australian Maritime Issues 2008*, PIAMA No. 27, Sea Power Centre - Australia, Canberra, 2009, p. 210.

242 Rahman, *The Global Maritime Partnership Initiative: Implications for the Royal Australian Navy*, p. 37.

243 Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars*, p. 241.

244 B Elleman, A Forbes, and D Rosenberg, *Piracy and Maritime Crime: Historical and Modern Case Studies*, Newport Paper No. 35, Naval War College Press, Newport, 2010, p. 235.

245 'Australian Airpower Controversy', *Defense Industry Daily*, 20 March 2008, <http://www.defenseindustrydaily.com/australian-air-power-controversy-f35-and-super-hornets-under-fire-03065/> 28 June 2010.

246 Information obtained from US Navy PEO C4I, International C4I Integration (PMW 740) on May 06, 2013.

247 The three Combined Task Forces (CTF) in the Mideast are: CTF 150, which is responsible for maritime security operations (MSO) – essentially counter-terrorist operations – in the Gulf of Oman, Gulf of Aden, Indian Ocean, Red Sea and Arabian Sea; CTF 151, which is responsible for counter-piracy operations in the Gulf of Aden and off the Somali coast; CTF 152, which conducts MSO in the Arabian Gulf.

248 The National Research Council, *Maritime Security Partnerships*, 2008, p. 75.