At the Crossroads of Cyber Warfare: Signposts for the Royal Australian Air Force

GRADUATE PAPER FROM THE
USAF SCHOOL OF ADVANCED AIR AND SPACE STUDIES

CRAIG STALLARD

At the Crossroads of Cyber Warfare:

Signposts for the Royal Australian Air Force

Disclaimer
This publication is presented by the Department of Defence for the purpose of disseminating information for the benefit of the public. The Department of Defence does not guarantee and accepts no legal liability whatsoever arising from or connected to the accuracy, reliability, currency or completeness of any material contained in this publication.
The content and views expressed in this publication are the author's own, and are not in any way endorsed by or reflect the views of the Department of Defence, or the official policy or position of the United States Government or Department of Defense, the United States Air Force or the Air University. The Department of Defence recommends that you exercise your own skill and care with respect to the use of this publication and carefully evaluate the accuracy, currency, completeness and relevance of the content for your own purposes.
This publication is not a substitute for independent professional advice and you should obtain any appropriate professional advice relevant to your particular circumstances.

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

National Library of Australia Cataloguing-in-Publication entry

Author: Stallard, Craig, author.

Title: At the crossroads of cyber warfare : signposts for the Royal Australian Air Force / Craig Stallard.

ISBN: 9781925062076 (paperback)

Subjects: Australia. Royal Australian Air Force. Cyberspace operations (Military science)--Australia. Air power--Australia. National security--Australia.

Dewey Number: 355.070994

Published by:
Air Power Development Centre, Department of Defence, PO Box 7932
CANBERRA BC ACT 2610, AUSTRALIA
Telephone: + 61 2 6128 7041 | **Facsimile**: +61 2 6128 7053
E-mail: airpower@defence.gov.au | **Website**: www.airforce.gov.au/airpower

At the Crossroads of Cyber Warfare:

Signposts for the Royal Australian Air Force

by
Wing Commander Craig Stallard

Copy of a Thesis Presented to the Faculty of the School of Advanced Air and Space Studies Air University Maxwell Air Force Base, Alabama

June 2011

The Air Power Development Centre

The Air Power Development Centre (APDC) was established by the Royal Australian Air Force in August 1989 at the direction of the then Chief of the Air Staff. Originally known as the Air Power Studies Centre, it was renamed the Aerospace Centre in 2000 and then became the Air Power Development Centre in 2004.

Its function is to promote a greater understanding of the proper application of air and space power within the Australian Defence Force and in the wider community. This is being achieved through a variety of methods, including development and revision of indigenous doctrine, the incorporation of that doctrine into all levels of RAAF training, and increasing the level of air and space power awareness across the broadest possible spectrum.

Over the years the APDC has evolved into an agency that provides subject matter expertise for air and space power education, and has a well-developed publication program. The Office of Air Force History (formerly known as the RAAF Historical Section) was amalgamated with the APDC in 1997.

Comment on this paper or inquiry on any other air power–related topic is welcome and should be forwarded to:

The Director

Air Power Development Centre
F3-Ground Floor
Defence Establishment Fairbairn
PO Box 7932
CANBERRA BC ACT 2610
AUSTRALIA

Telephone: + 61 2 6128 7051
Facsimile: + 61 2 6128 7053
Email: airpower@defence.gov.au
Website: www.airforce.gov.au/airpower

Foreword

One of the most important outputs supported by the Air Power Development Centre is the encouragement and invigoration of air power debate in the Australian context. Papers authored by RAAF students at the USAF School of Advanced Air and Space Studies are published by the Centre with this intent: to foster air power debate and through this debate challenge current ways of thinking.

This paper by then SQNLDR Stallard was written in 2011. Since the paper was written some of the issues addressed by Craig have evolved: a National Security Strategy and a new Defence White paper were both published in 2013. The Defence Signals Directorate has become the Australian Signals Directorate, which still houses the Cyber Security Operations Centre.

Nevertheless, Craig's paper addresses issues and makes arguments that are germane to addressing contemporary Air Force (and Defence and Government) cyberspace capabilities. Cyberspace is here to stay and its influence and impact on the generation, application and sustainment of air power can and will only increase.

I commend this paper to you as an insightful and relevant addition to the debate on the impact, use and importance of cyberspace in both the air power and Air Force contexts.

Group Captain Peter Wood, CSM
Director, Air Power Development Centre
October 2014

Preface

This paper is a copy of a thesis presented in June 2011 by Squadron Leader Stallard to the faculty of the School of Advanced Air and Space Studies, Air University, Maxwell Air Force Base, Alabama, for completion of graduation requirements.

The Air University has given formal approval for the APDC to reproduce this paper. The document is essentially the same as that presented to the School of Advanced Air and Space Studies, with only minor editorial changes to reflect Australian and ADF spelling and terminology.

A copy of the edited paper was sent to the author for comment and endorsement before publication.

Keith Brent
Editor
Air Power Development Centre
Canberra

September 2014

About The Author

Squadron Leader Craig Stallard is a member of the Royal Australian Air Force. Enlisting in 1982 and commissioned in 1988, his postings have included Nos 36 and 37 Squadrons as a navigator flying E and H model C-130 Hercules, and he has operational experience from *Desert Storm* to current day Afghanistan and Iraq. He undertook duties as the RAAF liaison officer at Central Command Air Forces (CENTAF) in the lead-up to Operation *Iraqi Freedom* before moving to the Combined Air Operations Centers (CAOCs) at Prince Sultan Air Base and Al Udeid for the kick-off and initial operational period.

As a Flight Commander at No 36 Squadron, he deployed to Indonesia as C-130 Detachment Commander during the initial stages of the 2004 tsunami relief effort and led a C-130 deployment to the Middle East in 2005. He has filled a number of staff positions at the wing, group, and Air Force Headquarters levels. Squadron Leader Stallard completed the USAF ACSC as a student in 2009 and remained on faculty for next 12 months as an instructor in the Department of Joint Warfighting.

Acknowledgements

I would like to acknowledge several people without whose support I would never have gotten off the ground with this study. I want to thank Group Captain Rick Keir for providing me the direction to steer this thesis, and Wing Commander Ralp Brown (RAF) and Squadron Leader Duncan Scott for affording me a look behind the curtains of cyber organisations in the United Kingdom and Australia.

I am grateful to thank Colonel Michael Kometer for his insight into the vagaries of command and control. I do not think there is a better person to advise on the tangled mess of centralised versus decentralised control of combat air power.

I especially want to thank Dr Stephen Chiabotti, who endured my colonial grammar and pushed me to write at a level beyond where I ever considered possible.

Most importantly, I thank my wife and son, for enduring the months of my isolation locked up in the depths of my study. Our lost family time can never be replaced, but you have my eternal gratitude for helping me through this marathon. This project truly was a team effort and I dedicate this thesis to them.

Abstract

This thesis provides signposts to guide the Royal Australian Air Force during its journey through the development of a cyber capability. As with most journeys, there are always multiple paths; the challenge is to choose a path that will deliver an effective cyber force with the available resources.

The emergence of cyberspace changed the character of war in ways Clausewitz could never have imagined. Cyber violence transcends the physical environment, creating effects on an adversary's warfighting capabilities as severe as a kinetic weapon. Uncertainty, the fog that envelops all aspects of conflict, remains ever-present; however, cyber enables commanders greater situational awareness, shifting the shade of fog from opaque to translucent. The ambiguities of identity and effects that exist in cyberspace juxtapose with the speed and span of cyber operations, reducing, but not eliminating, uncertainty.

The Australian Government's 2008 National Security Statement shaped the national cyber environment and raised the profile of cyber within the 2009 Defence White Paper. With new-found direction to pursue cyberspace as a warfighting domain, the Royal Australian Air Force is looking to move forward on the development of a cyber force but faces numerous hurdles in its path. At the forefront of these hurdles is an appreciation of just what effects the Air Force seeks from cyberspace. The development of a concept of operations would be a significant signpost to guide the shaping of a cyber force. At the heart of this force will be personnel—air-minded cyber specialists who will plan, coordinate and integrate cyber operations in support of air power. However, to raise, train and sustain an air-minded cyber force is an undertaking that requires long-term commitment and support from the senior Air Force leadership, without which an effective cyber capability for the Royal Australian Air Force will be unattainable.

The effects of cyber operations are real, and permeate across all warfighting domains. If the Royal Australian Air Force is to fulfil its responsibility to deliver air power in the defence of Australia, it must honour the cyber threat and accelerate its journey to develop a cyber force.

Abbreviations And Acronyms

ADF	Australian Defence Force
ADFA	Australian Defence Force Academy
AOC	Air Operations Centre
APDC	Air Power Development Centre
CERT	Computer Emergency Response Team
CNA	computer network attack
CND	computer network defence
CNE	computer network exploitation
CNO	computer network operations
CONOPS	concept of operations
COPT	Cyber Operational Planning Team
CSOC	Cyber Security Operations Centre
DSD	Defence Signals Directorate
IA	information assurance
ICBM	intercontinental ballistic missile
ISR	intelligence, surveillance and reconnaissance
JFACC	Joint Force Air Component Commander
JFC	Joint Force Commander
JOPP	Joint Operation Planning Process
JSF	Joint Strike Fighter
JTF	Joint Task Force
NCW	Network Centric Warfare
OODA	observe, orient, decide and act
RAAF	Royal Australian Air Force
RAF	Royal Air Force
SCADA	Supervisory Control and Data Acquisition
UK	United Kingdom
US	United States
USAF	United States Air Force
WMD	weapons of mass destruction

Contents

Figures

Chapter 1

Introduction

The Royal Australian Air Force (RAAF) has just begun its journey of developing a credible cyber force. Never normally shy about embracing new technologies to enhance the capabilities of air power, the RAAF has, however, made little progress in raising, training and sustaining the type of workforce needed to operate effectively in the cyber environment. Perhaps it is because cyber is just emerging as a warfighting domain, and the RAAF is looking for guidance from the Joint Operations Command; after all, the Air Force is inherently a joint fighting force. Maybe it is looking to develop a concept of operations that will steer the development of a cyber force. Alternatively, a focus on the kinetic applications of air power may have drawn attention from an appreciation of how a cyber attack could influence the nation and the RAAF's ability to deliver air power. The following brief tale provides an insight into what Australia, the Australian Defence Force, and the RAAF could face in a few years if they do not follow the signposts to develop a cyber future.

A tale of chaos reigns supreme

Picture a liberal-democratic country that operates within the bounds of regional norms. The population accords the responsibility for security to the government and pays taxes to fund the undertaking. The military is delegated the tasks of protecting the country and population from any attacking forces. Air, sea, land, space and cyberspace are the avenues through which an opposing force can traverse its borders to attack the population and their treasures. The military fields an army, navy and air force as the means of protection. These services control the domains in their region and block any opponent's army, navy, air force, or space capabilities from getting through to the country. But what about cyberspace? The military bears the responsibility for maintaining the integrity of the air, land, sea and space environment, and shares joint custody of the security of cyberspace with the government, the private sector and the population. The government has allowed the private sector and individuals to hold the responsibility for securing their portion of cyberspace. The population generally appreciates this

because they rely on cyberspace for nearly everything in life and want continued unfettered access.

Chaos begins. The morning of 25 November 2015 starts like any of the days over the past few months. The second global economic crisis in five years has affected every country in the region, with the cost of living increasing, trade decreasing, and a growing imbalance in wealth between regional countries. Our country is affected, but not as much as others are in the region. Our military has been able to repel the few military maritime and air intrusions, with the army defences strong but untested. No regional power has an offensive space capability, so that is not an area of contention. Suddenly all the automatic teller machines in the country stop working. The population complains to the banks, which raise their hands in exasperation, indicating it is not their fault. Next, traffic lights malfunction for 30 minutes or so, and then fail altogether. Rapidly, intermittent faults spread over the power grid, water control systems, air traffic control, and the stock exchange. Without a stable power system, information systems are disrupted. Citizens trying to access private-sector and governmental websites find the servers have crashed.

Air Force in chaos. The Air Force tries to scramble its fighters to provide a defensive air umbrella in case this cyber attack is a prelude to a ground invasion. But the air base refuelling system does not respond to computer commands to transfer jet fuel from the storage area to the flight line, so the jets have insufficient fuel to fly combat patrols. This would have been inconsequential anyway as the squadron's planning systems appear corrupted, and the data used to synchronise the aircraft's communication and weapon systems cannot be transferred from the computer systems onto the aircraft. Even if the fighters could get airborne, they could neither speak to anyone nor target their weapons on anything. The maintenance flight is wondering why they have received boxes of toys from FEDEX, and the local hospital is catching their head with all the boxes of engine, radar and radio parts that turned up in their shipping dock. Air defence radar units are reporting clear screens, while the air traffic control tower is telling the command post that civil airliners are circling overhead requesting permission to land. Even the instrument landing systems are malfunctioning. The military has combat forces at the ready, but with limited combat capabilities.

The Supervisory Control and Data Acquisition (SCADA) system that monitors and directs the country's primary dam facilities sends uncommanded signals to open the floodgates, creating widespread damage to crops and buildings. The military tries to assure the government and population that the country's air, sea, space and land environments are intact, so there is no physical threat to the country; news of the floodwater did not reach them. However, with the country's information systems disrupted, the message is difficult to get out and general panic erupts.

The military and the government rapidly establish they are under a cyber attack from an unknown actor. Because the military and government are responsible for their own cyber security, the majority of their essential information systems are protected and functional. However, it is quickly apparent to both organisations that many of their capabilities are degraded to varying degrees because of reliance on information systems housed in the private sector. Power, petrol, telephones, BlackBerries, and the Internet are just some of the commercial items the military and the government rely upon for the conduct of their activities. Despite the efforts of the military and government, instead of being a steadfast barrier like those of the other domains, the cyber firewall is constructed of chicken wire instead of steel. The country learnt a valuable lesson known to football coaches for generations: the effectiveness of defence is only as good as the weakest element.

What happened and who is to blame?

In the aftermath of the attack on the country, the finger of blame needed ice as it was pointed in so many directions. The military and government held up their records indicating that even though their information systems were attacked, the information itself remained relatively intact, even if it was inaccessible. The private sector acknowledged that their security systems were found wanting, but they will be addressed and will do better in the future. The population, many of whose computers were used in the botnet attack, is still asking questions of responsibility. After all, was the country not attacked, and is it not the responsibility of the government to provide security of the country? Should the population expect protection from any form of attack from an outside actor? Are there some forms of external attack from which the population must defend itself? If so, can the population legally respond against the other country or actor in self-defence?

ADF and cyber. What is the role of the Government and the Australian Defence Force (ADF) in the conduct of cyber operations that support the national security strategy? The release of the 2009 Defence White Paper, the National Cyber Security Strategy, the opening of the Cyber Security Operations Centre (CSOC), and the standing up of the Australian National Computer Emergency Response Team (CERT) go a long way to addressing many of the questions in the scenario.

The missing link. What is yet to be addressed is the role the RAAF will have in the conduct of cyber operations at the national level, in the joint organisation, and internal to its Service activities. There is no question that cyberspace is critical to the conduct of national security, the sustainment of the private sector, and maintenance of lifestyle. Equally, cyber operations are essential to the RAAF capability to provide swift, decisive, and resilient air and space power for Australia's security; and to maintain the respect of the Australian population and Government, as well as foreign audiences.

The road to cyber awareness

For more than three decades, global military forces have engaged in some form of digital warfare. As with all modern militaries, the ADF embraced the use of computers across all operational levels, including management, acquisition, logistics and the entire spectrum of its operations. The ADF as a joint organisation, and the RAAF as a Service, consider operations in the cyber domain integral to the nature of their core functions. In 2002, the ADF published its doctrinal approach to warfare (*Force 2020*) in which it foresaw the importance of transitioning from a platform-centric organisation to a force focused on network-enabled operations. This vision of the future, conceptualised in the ADF's *Network Centric Warfare (NCW) Roadmap* issued in 2007, sought to transition the Australian military from a network-aware to a network-enabled force by 2014. While *Force 2020* and the *NCW Roadmap* provided guidance on platforms, they provided little insight into a priority or structure for the ADF or the RAAF in the conduct of cyber warfare. The 2009 Defence White Paper provided some clarity by identifying cyber warfare as critical to the maintenance of national security, but left open the most important issue: should cyber warfare be a joint engagement or a Service-oriented fight? The RAAF, while developing into an effects-based force, struggles to emerge from its history as a platform-centric, kinetic-focused organisation. As such, the RAAF has yet to develop a coherent plan for where cyber warfare fits into its warfighting approach and what its role will be in the ADF's cyber warfare organisation.

Research question

How should the Royal Australian Air Force develop its role in Australian Defence Force cyber warfare operations?

Thesis overview

This thesis steps through a number of areas that are essential to understanding how the RAAF can develop a cyber force that supports its air power needs. Like any journey, there are a number of milestones to reach, and in the Air Force's case, these are obtained through an appreciation of the various environments that shape its cyber requirements. To answer the thesis question, the research will investigate command and control in cyberspace and provide the reader with an overview of cyber and its relation to information operations. The role the RAAF should take in cyber warfare is shaped by Australia's security strategy and, in particular, the most recent Defence White Paper and the National Cyber Strategy. From these documents, the research will develop a picture of cyber in the Australian military with insights from its international partners, the United States and the United Kingdom. It will then build an organisational framework around the RAAF's responsibilities to raise, train and sustain air power capabilities to

bracket the considerations required to build a cyber workforce. This analysis will enable a series of recommendations for the direction the RAAF should take in its future development of cyber warfare.

Chapter 2. Command and control in cyberspace requires a shift in thinking from the kinetic understanding of violence to a broader appreciation of violence as an effect rather than a physical action. Violence is often espoused as an innate tendency of war, but the emergence of the cyber domain brings into question whether violence should only be in the province of the physical. The expansion of cyber technology has for some warriors provided a promise to lift the fog of uncertainty that has cloaked the true picture of battlefield operations. However, uncertainty is omnipresent in war and commanders must embrace the chaos inherent in conflict. Cyber does not remove uncertainty; rather, it provides the opportunity for greater rationality in decision-making because of enhanced situational awareness. But improved awareness brings with it the debate on centralisation of control—the 5000-mile screwdriver remote commanders can now wield through the marvels of cyber technology. Cyberspace is enabling greater flexibility to the commander in the control of his forces, but it is best viewed as a medium that allows greater adjustment of centralisation rather than a reason to take over just because you can.

Chapter 3. Appreciation of cyber warfare's influence on air power requires an understanding of the terminology specific to the cyber domain. Land, air, sea and space are firmly entrenched as warfighting domains, but accepting cyberspace as a separate and unique domain is critical to success in the modern battlefield. The problem is that for nearly every cyber-related piece of doctrine or academic publication there is a different definition for cyberspace. Settling on an agreed-upon meaning will make it easier to identify where cyber fits into the hierarchy of information that runs from data through to wisdom. Cyber is centred on the exchange and processing of information, thus cyber permeates throughout information operations. The RAAF must accept that computer network operations are growing in complexity beyond what was envisioned in doctrine's understanding of information operations. Issues such as the attribution of a cyber attack make development of cyber deterrence difficult and complicate targeted response. However, balanced against the challenges are the significant benefits cyber offers to the warfighter. The RAAF is embracing Network Centric Warfare as a process to improve the decision-making cycle. It is within this process where the possibility exists to lift some of the fog that is omnipresent in conflict. Network Centric Warfare is not the same as cyber operations, though many core features operate through cyberspace. In the development of a cyber force, the RAAF needs to be aware of the differences in these functions if it is to develop an effective cyber capability.

Chapter 4. Each country approaches national security from a different perspective, and Australia's geographic and strategic environment shapes its approach to

cyber security. The Prime Minister's 2008 National Security Statement provided a launching pad for a national approach to cyber security. The Prime Minister's statement formed a nexus between the broader national Cyber Security Strategy and the ADF's cyber strategy embedded in the 2009 Defence White Paper. The Government made it clear that private and public sectors, along with the operators of critical infrastructure, were responsible for the security of their information systems. However, under the Department of the Attorney-General, a number of initiatives, such as the Computer Emergency Response Team and Trusted Infrastructure Security Network, would provide support and information to help better protect the non-government entities from the impacts of cyber attack. Responsibility for government cyber security, including those of the ADF, rests in the Cyber Security Operations Centre, an element of the Australian Signals Directorate. If the RAAF wants to influence the development of future cyber capabilities it needs to grow its cyber representation within the Australian Signals Directorate.

Chapter 5. So what does cyber mean to the ADF? Like most questions, the answer depends on whom you ask. The Department of Defence differentiates responsibilities into two camps; security of government information systems and computer network operations in support of military operations. The ADF appreciates the importance of cyber to its future effectiveness as a fighting force, though it is lagging in efforts to raise a cyber force. Make no mistake, cyber operations are inherently joint; but there is little movement in the development of any effective joint cyber capability. The ADF has embraced Network Centric Warfare, in which cyber is a key ingredient, but this is a long-term transformation of its entire warfighting system to enable it to fight as a whole rather as individual parts. From the Service perspective, the RAAF has to grapple with the question, 'is cyber superiority possible?' Absolute superiority is probably not possible; however, cyber operations can enable asymmetric advantage in decision-making that can be the decisive factor in an air campaign. The key to cyber supporting air power is the development of an air-minded cyber force. Cyber specialists can be employed to support the security of government information systems, but the Air Force needs cyber operators with the insight into what is relevant to the air fight. Air-minded cyber operators can integrate into the air component planning teams and provide the air perspective in a joint cyber environment. Target development, collateral-damage assessment, weaponeering, and collection management are all as important to cyber operations as they are in the kinetic realm, and only cyber specialists with a grasp of air power can do justice to these functions. Without an air-minded cyber force, the RAAF will continue to become increasingly vulnerable to cyber attacks.

Chapter 6. The RAAF is responsible to the Australian people for the delivery of air power in the defence of the nation. Without an effective cyber capability, the ability to deliver on this responsibility is questionable. However, building a cyber

force will be neither cheap nor easy. Fiscal pressures will constrain the capacity to conduct the full range of cyber operations that may be required. Alongside budgets and equipment needs, is a requirement to adjust its force structure and modify the organisation. Competing mission requirements will place pressure on redistributing the workforce required to build a cyber force. Perhaps the easiest but most debated element of raising a cyber force will be where it fits inside the organisation. Cyber warfare is more than information operations, with a separate mission, distinct skill sets, and a different focus in the support of air power. The RAAF will need to stand up a separate and unique cyber squadron, tasked with training its cyber force, developing air-specialised cyber capabilities, and liaising with the other Services and joint cyber elements for synchronisation of effort. Critically, the cyber squadron will be the nucleus for the cyber operational planning teams (COPTs) that will be the sharp end of the RAAF cyber capability. COPTs will conduct the planning, synchronisation, coordination, and in some cases execute cyber operations in support of air tasking. Air-minded cyber specialists will integrate into the Joint Operations Command and any Joint Task Force cyber teams to provide the air perspective to operational planning activities.

The greatest challenge in developing a cyber force will be raising, training and sustaining the people who form the core of a capability. The Air Force needs a cyber force now, because conflict in the cyber domain is not something the Air Force faces in the future, it is a reality today. A multifaceted recruiting effect, targeting officers, airmen and civilians, is required to build the cyber force. Technical and academic curricula across most RAAF training institutions should reflect some element of cyber, just as air power is fused into most training and education. The Air Force needs to shape, train and develop the cyber mind of not only its specialists, but also the senior leadership and broader RAAF population. Cyber is not a passing fad; it is not a technology, but an emerging warfighting domain that must be embraced if future air power is to be effective.

Chapter 2

Command and Control in Cyberspace

The effect of the medium on war

Throughout history, the arrival of a new technological age has heralded a shift in the character of war. The invention of the train with its mass transportation capability during the industrial revolution enabled a growth in armies that went from forces measured in thousands into armies of hundreds of thousands, and eventually millions. The development of the aeroplane, with its speed and range, added the vertical dimension to the battlefield, forever changing the mobility, firepower, and communication characteristics of manoeuvre warfare. The space age, with missiles that cross continental divides in under 30 minutes, and satellites that provide persistent surveillance of battlefields, transformed the concepts of global response and battlespace awareness. The information age, with the advent of cyberspace, heralded changes in decision-making time lines from weeks, days, hours and minutes, into operations measured in seconds. As the character of war has changed, so have the concepts of command and control. This chapter argues that while the information age has not altered the nature of war, the influences of cyberspace have changed both the character of war and the practices of command and control.

There are many types of war, but all wars share the same nature, or as espoused by Clausewitz, the innate tendencies of violence, hatred and enmity.[1] Each tendency is intrinsically separate, but inherently linked to the others to form a phenomenon that endures as the nature of war. These tendencies are constants in every type of war, even when the characteristics of each war change. No two wars occur for the same reason or are conducted the same way. The character, or distinguishing quality of a war, is shaped by influences such as the belligerents' politics, morals, religion, geography, economics, technical capabilities, or security environment.

1 Carl von Clausewitz, Michael Eliot Howard & Peter Paret, *On War*, rev. ed., Princeton University Press, Princeton, NJ, 1984, p. 89.

The Crusades, the series of religiously sanctioned military campaigns during medieval times, are distinguishable from World War I, not so much by the level of violence, but by the differing catalysts for conflict—religion versus geopolitics. Similarly, the Vietnam War and Operation *Desert Storm* were both preventive wars, distinguishable by their differences in politics, geography and particularly technology. David Lonsdale argues chance, uncertainty, and the ever-present friction in war ensure that 'war is far from being a wholly predictable activity', thus the character of a war can rarely be accurately foreseen.[2] Lonsdale further asserts that 'policy gives birth to the child of war', and stands as the most influential tendency in the nature of war; without policy, war would be 'just mindless violence.'[3] Violence is the manifestation of human nature to contest an opposing will. Lonsdale asserts that the human factors such as emotion, concern, morality and fear shape the preparation and conduct of war.[4] For these reasons, no two wars are ever the same. Conflicts are fought for different ends, in different ways and with different means. They share some degree of hatred and enmity between peoples or governments, and in all cases, forces clash in violent ways.

Violence

Command-and-control practices do not focus on hatred and enmity, though these tendencies influence command performance, but on the execution of violence, as this is the primary act performed by the military on behalf of the people and the government. Napoleon may have encouraged hatred and enmity in his troops towards the Prussians, the British and most everybody in Europe, but it was through the conduct of command and control that he applied violence with his forces. The violent clash of force is what distinguishes war from the other political means of intercourse. Throughout history, violence characterised the actions that caused death or injury to populations and forces, and widespread destruction to infrastructure and equipment. As Von Moltke asserted, 'War is a rough and violent business … hardly a single family escapes the common suffering.'[5] From the first tribal wars between primates, through to the start of operations in support of the Global War on Terror, the physical dimension has been the cauldron for violent actions; the emergence of cyberspace challenges this belief.

Cyberspace challenges the traditional perception of violence in war, but the violent nature of war continues unaltered. War, as espoused by Clausewitz, is 'an act of

---

2 David J Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, Cass Series: Strategy and History, Volume 9, Frank Cass, New York, NY, 2004, p. 39.

3 ibid., p. 28.

4 ibid., pp. 36–39.

5 Helmuth Moltke & Daniel J Hughes, *Moltke on the Art of War*, Presidio Press, Novato, CA, 1993, pp. 22 & 26.

force to compel our enemy to do our will'.[6] Clausewitz viewed force as a pulsation of violence in the physical realm because, aside from the moral force, which he considered had no existence in war except through government and law; there was no other type.[7] To Clausewitz, the notion of violence by any other means than physical was as foreign a concept as was the idea that space was a domain available for exploitation in war. There was no technological or conceptual framework to consider violence in any other way except in a duel of armies or navies. From Emperor Napoleon Bonaparte through to General Norman Schwarzkopf, warfighting was about defeating the enemy on the battlefield through physical conflict or attacks on the adversary's population and infrastructure. During the Battle of the Somme, Field Marshal Douglas Haig threw wave after wave of his forces across the trenches at German machine guns in an effort to achieve victory on the battlefield. To secure an entry point into Europe, General Dwight Eisenhower had little option than a physical invasion through French beaches. General Schwarzkopf's plan for victory in Operation *Desert Storm* was to destroy Iraq as a military power, and that required the physical destruction of the Iraqi Republican Guard.[8] Up to the development of cyber operations, physical force was the paradigm under which war was conducted. However, just as the concept of the battlefield changed with the advent of the aircraft, the interpretation of violence should change with the emergence of cyberspace. Violence is characterised by a marked or intense change in the character of the targeted entity.[9] An action's effect, whether caused by physical contact or by informational influence, is the most important factor in determining violence.

Cyber Violence. A cyber attack can have an intense effect on an adversary's warfighting capabilities—just as severe as a kinetic weapon—which should be construed as violence. During war, trains are frequently destroyed through the bombing of marshalling yards or rail bridges. A cyber attack on a rail-switching unit can send trains on collision courses with violent effects similar to physical attack. A successful cyber attack experiment on a power generation system by the Department of Homeland Security demonstrated the ability of cyber operations to cause the violent destruction of a generator unit.[10] The cyber attack

---

6 Clausewitz, Howard & Paret, *On War*, p. 75.

7 ibid., pp. 75 & 87.

8 Colonel Richard T Reynolds, USAF, *Heart of the Storm: The Genesis of the Air Campaign against Iraq*, Air University Press, Maxwell Air Force Base, AL, 1995, p. 107.

9 Merriam-Webster, *Merriam-Webster's Collegiate Dictionary*, 11th ed., Merriam-Webster, Inc., Springfield, MA, 2003, p. 1396.

10 Jeanne Meserve, 'Mouse Click Could Plunge City into Darkness', CNN online, viewed 6 February 2011, <http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html>. YouTube video of the generator can be accessed at <http://www.youtube.com/watch?v=fJyWngDco3g>, viewed 6 February 2011.

caused the generator to vibrate out of balance and cause a catastrophic failure of the generator turbine. Experience during the Los Angeles riots in 1992 and the civil unrest following Hurricane Katrina demonstrated how rational people turn violent given a threat to their lifestyle. A large-scale cyber attack on the US financial system could have such a broad effect on the lifestyle of the average American that the attack would have to be considered violent.

Cyber attacks can have violent effects. Thus with the advent of cyberspace, the Clausewitzian concept of the violent nature of war remains unchanged, but the violent character of war has evolved. War remains violent, whether conducted in the physical or ethereal realms, but the speed, reach, effects and ambiguity of an attacker's identity in cyber operations has altered the conduct of war.

Cyber War

Just as aviation transformed the character of war, cyberspace is altering its face again. Billy Mitchell, in his monograph on air power advocacy, *Winged Defense*, heralded the passing of the continental era, where power was consolidated on the ground, to an aeronautical era where the air domain would determine the destiny of the human race.[11] A bold prediction, but in the 100 years preceding the publication of his book, although land battles had increased in destruction, they were slow in gaining strategic outcomes.[12] Mitchell foresaw the exploitation of the air domain as the next evolutionary step in the process of warfare. As the range of an arrow reduced the two-dimensional effectiveness of an army equipped with only clubs and swords, the speed, range and payload of aircraft changed conflict on land and sea.[13] The air domain enabled a third dimension for the exercise of force, just as space provided a fourth dimension to exploit. Cyberspace, as a domain in its own right, adds a fifth dimension to project violence upon an adversary. Cyber weapons exist in the form of software and influence the adversary's networks to varying degrees. Full details of the cyber attack on an Iranian nuclear facility using the Stuxnet worm in 2010 are not likely to be publicly released, but media reporting indicated that Iran lost control of critical systems and had little appreciable awareness that they were under attack.[14] It is not difficult to conjecture that other civil nuclear control components, such as

---

11 William 'Billy' Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power–Economic and Military*, University of Alabama Press, Tuscaloosa, AL, 2009, p. 3.

12 Mitchell's observation of the slow moving and brutal nature of World War I land battles, from aircraft with speed and range never previous available to combat forces, was a driving force behind his conviction that air power was the future of warfare.

13 Mitchell, *Winged Defense*, pp. 15–16.

14 'The Stuxnet worm; Yet to turn', *The Economist*, 16 December 2010, viewed 6 February 2011, <http://www.economist.com/node/17730556>.

cooling-rod valves or pumps, could be vulnerable to attacks using software, with ramifications comparable to the Russian Chernobyl disaster of 1986. The impacts of cyber attacks may resemble those from other domains, just as the effects of an artillery shell and a bomb from an aircraft can appear the same even though the delivery method differs substantially. Commanders who fail to appreciate the different face of war that cyberspace puts forward will lose the operational advantages cyber operations offer and struggle to respond to the implications of a cyber attack.

The uncertainty principle

One of the key implications of cyberspace on command-and-control practices is the ambiguity that is inherent in cyber operations. Attackers can deliver malicious software across networks at the speed of light, with the time between initiation and execution of an operation limited only by the program's design, network security, server infrastructure, and routing access. Like mines or cluster munitions, software bombs can be designed to take immediate effect or lie dormant waiting for a predetermined time or event. Unlike physical weapons, however, cyber operations are conducted in relative ambiguity because of the distributed nature of networks, making the identity and intent of the attacker difficult to determine. The 2007 cyber attack on Estonia, which crippled many of the Baltic nation's government, financial, media, and corporate websites, was linked to Russia due to the geopolitical environment, but the ambiguity of attribution made it impossible to officially blame any nation or organisation.[15] Software botnets, routed through multiple computer systems whose owners are unaware they are proxies to an attack, can measure in the tens of thousands and make tracing the source of an attack difficult. If the source of an attack cannot be attributed, who does a country target if it seeks retribution or looks to defend itself? Sun Tzu said that to achieve victory you must 'know your enemy', so if you cannot identify the enemy, upon whom do you focus your operation?[16] Gaining an awareness of enemy capabilities is fundamental to the practice of command and control. Commanders at all joint and component levels need to know who the enemy is so they can focus planning and targeting efforts to best effect and most directly contribute to achieving objectives.[17] Without an identity the integrity of

---

15 William A Owens, Kenneth W Dam & Herbert S Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Academies Press, Washington, DC, 2009, p. 173.

16 Sun Tzu & Samuel B Griffith, *The Illustrated Art of War*, Oxford University Press, New York, NY, 2005, p. 125.

17 United States Joint Chiefs of Staff, Joint Publication 1: *Doctrine for the Armed Forces of the United States*, Joint Chiefs of Staff, Washington, DC, 2007, p. IV-8.

the Joint Operation Planning Process (JOPP), a core element of US command-and-control practices, is placed at risk. Pivotal to the JOPP is the requirement to understand the objectives, intentions, capabilities and limitations of all actors within the operational environment.[18] The ambiguities of identity and effects that exist in cyberspace juxtapose with the speed and span of cyber operations to engender a high degree of uncertainty. Command-and-control practices need to adapt from the relative sureness of the physical domain to the uncertainty of the cyber domain if they are to remain effective in the new multidimensional battlefield that includes cyberspace.

Terminology. Terms, such as information dominance, real-time intelligence, or persistent surveillance, incorrectly suggest that cyberspace has the potential to lift the fog of uncertainty that has constrained the practice of war throughout history. Unfortunately, uncertainty will continue to exist to some degree because, even with the capabilities that cyberspace supports, inherent limitations in processing information and network infrastructure inhibit achieving a perfect battlefield picture. Infrastructure will improve as technical innovation occurs, but information, which lies at the heart of cyber operations, continues to permeate the fog of war. Information has been the difference between success and failure on battlefields for many a general officer. Commanders with the most accurate information on the enemy's force composition and position, as well as their own, are usually in the best position to exploit offensive opportunities and reduce defensive vulnerabilities. Information is, however, a double-edged sword. The vast amount of information flowing into a headquarters can overwhelm the ability to provide context and apply analysis to it; that is, inhibit the conversion of raw information into intelligence. Clausewitz gave little credence to intelligence because information could reach the command only through numerous interpretive filters due to the limited communications infrastructure of the time, increasing uncertainty.[19] Unfettered information is open to interpretation by the commander and staff, which at best can be a distraction from the functions of command (i.e., Predator crack) and at worst lead to poor decision-making. Uncertainty breeds in an environment with too much, too little, or unfiltered information.[20] Cyberspace is not the panacea that can lift the veil of uncertainty from a commander's eyes. However, properly managed, cyberspace can support building a better, though not perfect, situational awareness of the battlefield, which great commanders can then exploit.

---

18 United States Joint Chiefs of Staff, Joint Publication 3-60: *Joint Targeting*, Joint Chiefs of Staff, Washington, DC, 2007, p. II-1.

19 Clausewitz, Howard & Paret, *On War*, pp. 117–18.

20 Mr John Luddy, *The Challenge and Promise of Network-Centric Warfare*, Lexington Institute, Arlington, VA, 2005, p. 6.

Coup d'oeil. Cyberspace is a tool for a commander to cultivate Clausewitz's notion of the coup d'oeil, the inward eye, that enables the development of a picture of the battlefield, to conceptualise the strengths and vulnerabilities of the forces on both sides, and to make decisions better than those of the adversary.[21] Genius consists of a harmonious combination of elements, such as courage, intellect, coup d'oeil, determination, presence of mind, and boldness, in which one or the other may predominate, but none may be in conflict with the rest.

The ability to visualise the *big picture*, the strategic and operational view of a battle, appreciate opportunities, and have the intuition to exploit them in a timely manner, is enhanced by the networking effects of cyberspace. Real-time communications between commanders and their forces permits orders to be passed and intent to be transmitted, regardless of the geographic location of any of the actors. The Joint Operations Commander, located in Bungendore, can receive live briefings from the Joint Forces Commander in Afghanistan, with the same fidelity as the Air Operations Centre can receive directions from the Wedgetail mission commander. Cyberspace enables information to be compiled, disseminated and received almost instantaneously, enabling the commander to develop the *big picture* of the strategic, operational or even tactical environment.

However, Network Centric Warfare is a tool, not skill. It cannot make decisions, or reach inside the adversary's mind and broadcast intent. It will not make mediocre commanders great, but if properly exploited, can make good commanders better, and their forces more effective. Commanders' experience and talent, supported by cyberspace, are determinants for success or failure in the practice of command and control.

Command and control at the speed of light

Cyber operations shorten the time line between approval and effect, requiring command-and-control practices to become more flexible. Decision-making time lines for strategic maritime operations are measured in weeks, land in days, air in hours, and space in minutes, but for cyberspace operations, the time line

21 Clausewitz, Howard & Paret, *On War*, p. 102. Coup d'oeil refers to the quick recognition of a truth that the mind would ordinarily miss or would perceive only after long study and reflection.

to make a decision could be measured in seconds.[22] Like a physical weapon, the development of software destined for use in a cyber attack can take weeks or even months to a produce. Unlike its kinetic cousin, software is designed with a specific target in mind rather than a general type of target. This could be equated to a precision weapon designed to take out not a type of target like an aircraft bunker, but a specific bunker such as revetment 1A at an adversary's air base. A different weapon would be designed to attack revetment 1B. For a kinetic weapon delivered by an aircraft, the period from the execute decision to weapon-on-target is measured in hours, and limited by only platform type, transit distance, and adversary defences. With a cyber weapon, the period from decision to weapon delivery is measured in seconds. Both kinetic and cyber weapons may take time to negotiate an adversary's defences, but for air that can be measured in minutes, whereas for cyber the period can be seconds.

The implication for command-and-control practices, whether offence or defence, is a significant reduction in decision-making time lines. An adversary can close a vulnerability almost instantly, rendering a cyber capability impotent. Thus, the authority to conduct an operation may be required in a very short time. Equally, the opportunity to defend against a cyber attack may be only fleeting, as the adversary's software may attempt to bypass a firewall or corrupt some security protocols. Using kinetic decision-making practices in a cyber operation can lead to lost opportunities. Command-and-control practices must have decision processes that are compatible with the characteristics of cyber operations. Decision speed can be the difference between success and failure in a domain where cyber effects travel at the speed of light. The practices of command and control in cyber operations will differ for those in a kinetic operation. Understanding the character of command and control across the differing domains will be the difference between success and failure in any spectrum of war.

The conundrum of command and control

What is command and control? Are they separate functions? Can you have command without control? Where does the tenet of centralised control and decentralised execution fit in? Before appreciating the implications of cyberspace

22 For the maritime component, the response time to position a ship can be measured in weeks due to the speed of the ship and/or the transit distance. For land, manoeuvre or infantry elements can require days to implement an operation due to logistic requirements and unit relocation. Air has to transit to the target, thus the response time will vary depending on the proximity to the target. The hypersonic speed of ICBMs can result in only minutes available to respond to an enemy missile attack. Information over networks travels at the speed of light, thus cyber operations are only limited by the time for the program to initiate.

on these terms or phases, it is timely to define what they are and what they are not.

Command sits at the top of the hierarchical tree. According to the US bible of joint terminology, Joint Publication 1-02, command is 'the authority that a commander in the armed forces lawfully exercises over subordinates by virtue of rank or assignment'.[23] It is power, vested by a duly ordained superior onto a person holding a particular position, to use designated resources and 'for planning the employment of, organizing, directing, coordinating, and controlling military forces for the accomplishment of assigned missions'.[24] The essence and responsibility of command is laid out clearly in joint and Service publications, and generally not open to interpretation.

Command and control is therefore the exercising of the designated authority over assigned resources and forces to achieve a directed mission.[25] Martin Van Creveld simply states that command is a function that has to be exercised continually if the military is to exist.[26] He further asserts that the core functions of command, to feed and equip forces and conduct operations, are not subject to change.[27] However, as the environment and means vary, so will the way these functions are conducted. Command and control must therefore adapt to significant changes such as the emergence of cyberspace.

Control. Control is all about the power to plan, organise, direct and coordinate forces in order to execute a mission. Control exists at all levels of the spectrum of war, and it is at the discretion of the commander as to the degree of control imposed on subordinate commanders. How much control depends on factors such as the type of conflict, nature of the task, availability of resources, importance of the mission to the overall objective, strategic or operational consequences of tactical actions, or the level of risk the commander is prepared or authorised to accept. Understandably, the control of a nuclear mission is retained at a much higher level than a close air support (CAS) task. However, the degree of control of a CAS task will differ during an unlimited war than during a limited war due to the political sensitivity or strategic/operational consequences. The degree of control also changes across and within operational domains as the environment and mission change. Control in the air has different challenges than encountered

---

23 United States Joint Chiefs of Staff, Joint Publication 1-02: *Department of Defense Dictionary of Military and Associated Terms*, Joint Chiefs of Staff, Washington, DC, 2010, p. 65.

24 ibid.

25 ibid.

26 Martin Van Creveld, *Command in War*, Harvard University Press, Cambridge, MA, 1985, p. 5.

27 ibid,. p. 9.

on the sea; the control of a ground unit will be vastly different from the control of a cyber operation. Each domain is unique, and attempts to translate control across the differing environments have been a source of friction, ambiguity and confusion among the Services for generations. Control needs to be tailored to the operational domain, strategic consequences, available technology, and type of mission rather than a *cookie-cutter* approach.[28] So, if control is about the planning, organising, and direction of a mission, how much influence should the higher commander have on those subordinated to execute the task?

5000-mile screwdriver. With seemingly complete access to the battlefield picture via cyberspace, commanders can reach into the operational or tactical areas of operation and provide direction to subordinates executing the mission. With the advent of cyberspace came the 5000-mile 'command screwdriver'.

In some way, the practice of command and control has gone full circle since the Athenian era when generals directed the tactical execution of their units. As armies grew beyond the ability of a general to direct execution, leaders like Napoleon subordinated field commanders to execute strategic and operational intent. As the scale of war grew, field generals further subordinated control and the direction of execution to lower and lower echelon commanders. The size of the battlefield pushed operational planning to a headquarters well remote from the point of execution. By World War I, the era of generals like Robert E Lee directing the execution of a battle from a hillside had long passed. Units executed tasks based on mission orders and intent with little direct influence by a higher command. As communication technology advanced, higher echelon commanders were able to provide more guidance to those executing the mission. During World War I, field telephones allowed a remote headquarters to provide direction to units just before they commenced an attack. The use of portable radios during World War II allowed commanders in the immediate area of a battlefield to direct forces during the execution of a battle. The opening up of the space domain and advancements in cyber technology once again permitted the modern commander to direct a battle in the same manner as Alexander or Lee, but from a virtual hillside 5000 miles away. Networked communications allow commanders to tune the execution of a mission in real time, as if they were holding a 5000-mile screwdriver.

Unfortunately, the warriors executing the missions are feeling that screwdriver more and more in their back. One problem with this approach is a gap between what the commanders think they know and what is actually occurring in the battle. Local commanders have the benefit of a real-time appreciation of the

---

28 Lieutenant Colonel Michael W Kometer, USAF, *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower*, Air University Press, Maxwell Air Force Base, AL, 2007, p. 61.

battlespace and may have insight into local situations that electronic sensors cannot detect. Commanders who reach down into the operational or tactical environment can inhibit local commanders' ability to use initiative in the execution of their tasks.[29] The effect of cyberspace is to enable the direction of execution to move further away from the battle and more into the realm of control.[30] Cyberspace has reenergised the debate on the centralisation of control and execution.

Centralisation. Centralisation is not a binary phenomenon. The tenet of centralised control and decentralised execution is often lambasted as being inflexible because centralisation is viewed as either fully one way or the other—an on/off switch rather than a rheostat.[31] Centralised control is at one end of the operational spectrum and execution at the other. In reality, centralisation is a continuum where the degree of centralisation is determined by the type of conflict, the task, resource availability, importance of the mission to the overall objective, strategic or operational consequences, or acceptable risk. The elements of control, such as planning, coordination or direction, are conducted at varying levels of centralisation. Centralisation of control in domain changes as do the tasks within the domains.[32] The degree of control over a guided missile frigate will differ from that of a patrol boat. Because of air power's responsiveness and range, centralised control offers the potential to maximise the flexibility and effectiveness of air power through concentration of effort to integrate and synchronise effects.[33] The centralised direction of task execution will also vary as the controls vary. Labelling execution as decentralised does not automatically place the direction at the extreme low end of the continuum, but in a band.

---

29 Lieutenant Colonel Clint Hinote, USAF, *Centralized Control and Decentralized Execution: A Catchphrase in Crisis?*, Research Paper 2009–1, Air University Press, Maxwell Air Force Base, AL, 2009, p. 20.

30 Kometer, *Command in Air War*, pp. 101 & 16.

31 ibid., p. 34.

32 ibid., p. 37.

33 ibid., p. 33.

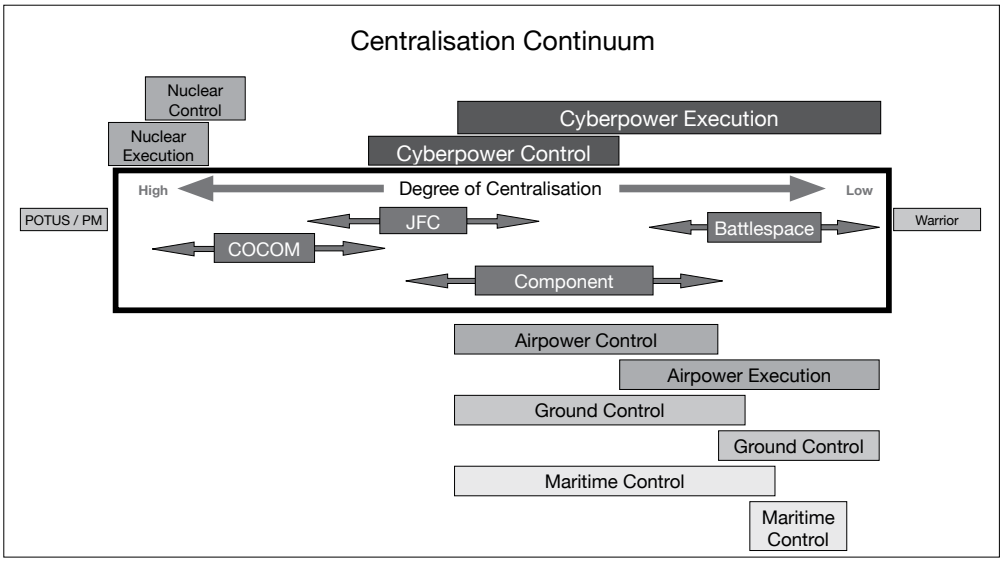

Figure 2–1: Continuum of centralisation[34]

As indicated in Figure 2–1, the direction of the execution of a cyberspace operation could vary from the unit level through to the Joint Force Commander, dependent upon the nature of the operation. There can always be a crossover between the degree of control and the level of centralised direction during execution. The command-and-control system, including those executing the task, needs to be adaptive to shifts in centralisation as the strategic and operational environment changes.

Command-and-control rheostat. The command-and-control organisation should be structured as an open system so it can respond to shifting levels of centralised control across different domains, changing operational environments, and adaptive, networked technology. Antoine Bousquet argues that the chaos of the modern battlefield requires the military to restructure towards a more complex, adaptive system that operates at the edge of chaos.[35] The more networked an organisation is, the flatter the hierarchy need be. This allows greater redundancy and creates self-organising units better equipped to react to the complexities in war. Uncertainty and disorder are central to the character of war, and an organisation willing to view conflict through a chaoplexic lens is better placed to

34 Source: Author's original work.

35 Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, Columbia University Press, New York, NY, 2009, p. 202.

respond to the unpredictability of an adversary.[36] The ability to scale the level of centralisation, combined with the battlespace awareness provided by Network Centric Warfare, synthesises the advantages of cyberspace with the realities of war.[37] Through Network Centric Warfare, commanders gain a broader and more persistent picture of the battlespace and make more timely decisions to support changes in the operational environment. Future networked operations would enable infantry patrols to engage with land, sea or air elements to respond to changing operational requirements without coordinating through intermediate headquarters. All commanders will be synchronised into the higher echelon's requirements and the broader operational picture, minimising centralised control, and enabling execution that is more responsive. Command-and-control practices need to be flexible and facilitate a 'rheostat' approach to the centralisation of control to gain the full benefits available from Network Centric Warfare.

Service perspectives. A large impediment to achieving more responsive command and control in the cyber age is the differing concepts of war held by each Service. Carl Builder argues that each Service views the other Services through different lenses, and worships at different altars.[38] To the Navy, independent command at sea is sacrosanct because it affords the commanding officer of a ship total responsibility for the actions of the crew and complete autonomy of action. The pervasiveness of cyberspace, while reducing uncertainty in the battlespace picture, enables higher commanders to tread where only ships' captains were allowed to, reducing the traditional freedom of action enjoyed on the high sea. The Army measures its effectiveness by its ability to put boots on the ground, and allows these boots to conduct operations within broad mission orders. Execution has a very low degree of centralisation, with units expected to use initiative to achieve desired objectives. To foster this initiative, control is exercised at the bottom portion of the centralisation continuum.[39] Cyberspace can be both a friend and foe to the Army's traditional concept of operations by enabling greater autonomy amongst networked units, or conversely allowing the hand of a commander to reach into the battlefield to redirect tactical operations. Builder espouses that the Air Force is all about technology and its toys, so it should be no surprise that cyberspace is embraced as a tool to maximise the efficiency of a finite allocation of its toys.[40] Adaptive centralisation of control is an entrenched

---

36 ibid., p. 200.

37 ibid., p. 233.

38 Carl H Builder, *The Masks of War: American Military Styles in Strategy and Analysis*, A RAND Corporation Research Study, The Johns Hopkins University Press, Baltimore, MD, 1989, pp. 17–22.

39 Hinote, *Centralized Control and Decentralized Execution: A Catchphrase in Crisis?*, p. 18.

40 Builder, *The Masks of War*, p. 23.

Air Force tenet. Cyberspace provides the opportunity for greater flexibility and reduced centralisation of control if required, as is needed during irregular warfare. However, centralisation of execution can also increase if the consequences of a mission warrant, as in the case of a high-value target.

Summary

While the character of war shifts with the tide of technology, the nature of war remains resolute. The emergence of cyberspace has come closest to challenging the notion of an immutable nature by expanding the concept of violence beyond the physical sphere. Violence as an effect, rather than as an action, brings into question some of Clausewitz's ageless principles of war, but rest assured his canons are safe, just interpreted for the current era. Equally, cyber does not alter Clausewitz's foundational axiom that war is the realm of uncertainty, there is just the ability make the fog a little less opaque.[41] While cyber can breed less uncertainty, its ability to enhance situational awareness across most reaches of the battlespace intensifies the debate on the centralisation of control and execution. Cyber allows the commander to reach out of the operational arena into the tactical lines (or cockpit) and manipulate control of what traditionally was the purview of the front-line warrior. Of course, there are pluses and minuses in every debate, and operational commanders bear responsibility for the outcome of any tactical activity, but the degree of control should depend on the operational and strategic environment, not just the capacity to act. Cyberspace facilitates the adjustment of control across the continuum of centralisation; the challenge for commanders is when and by how much to adjust the rheostat.

41 Clausewitz, Howard & Paret, *On War*, p. 101.

Chapter 3

Cyber 101

Every age has its own kind of war, its own limiting conditions, and its own peculiar preconceptions.

Carl Von Clausewitz

Warfare is the highest echelon of human conflict and involves the act of force (*means*) to compel an enemy to do our will (*objective*).[42] An increasing trend in academia, the media and doctrine is to label all functions the military performs as warfare, and cyber has not been immune. The ubiquity of cyberspace requires the Department of Defence to conduct cyber operations, in concert with governmental organisations and the private sector, during periods of both peace and war to support national strategic interests. Prior to open conflict, the military will shape the operational environment through operations that place the nation in a more advantageous position in comparison to potential adversaries. Many of these operations will be defensive in character, such as the employment of integrated air defence systems, maritime patrols, and in the case of cyber, robust network security systems. To be sure, in the event of conflict, the military will conduct warfare to meet its responsibilities of executing activities in support of national objectives.

Cyberspace is not solely the province of the military, with governmental organisations and the private sector heavily invested in its continued freedom for use. Warfare is the responsibility of the military, but all invested parties carry out cyber operations to some degree. Many of the strategic interests of these parties are captured in Amit Sharma's Clausewitzian interpretation of strategic cyber warfare, depicted in Figure 3–1. Warfare is the responsibility of the military, but

42 Edward Waltz, *Information Warfare: Principles and Operations*, Artech House, Boston, MA, 1998, p. 75.

as all parties undertake cyber operations in some form, this paper will use the use the phrase 'cyber operations' to describe most activities in cyberspace. Specifically, cyber operations include; cyber security, also referred to as cyber defence; cyber attack; and cyber support activities. This chapter will focus on the military aspects of cyber operations, all of which fall under the banner of information operations, specifically computer network operations.

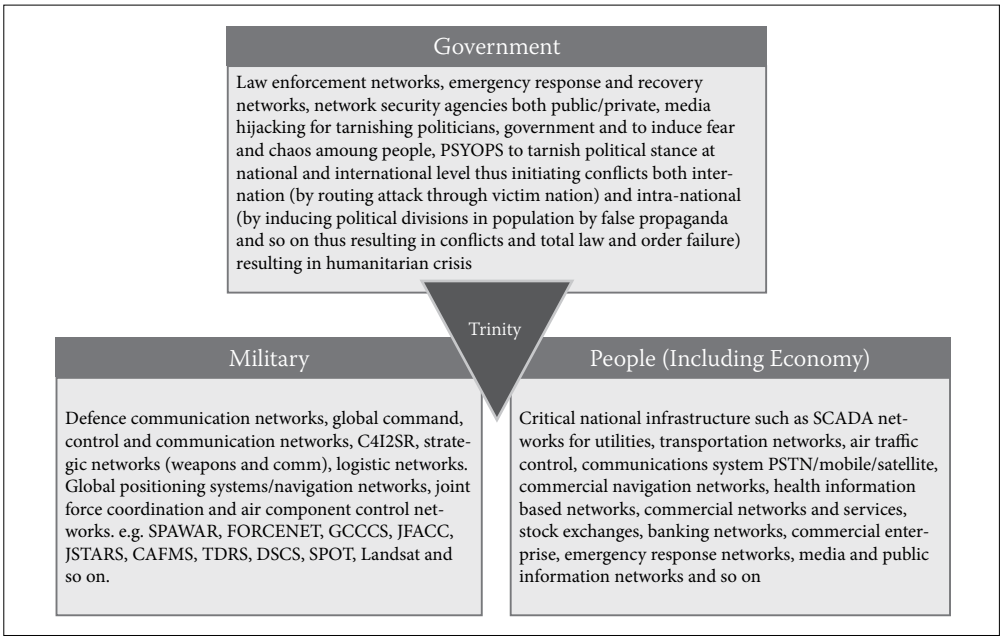

Figure 3–1: The notion of trinity in terms of strategic cyber operations[43]

Terminology. The complexity of the cyber domain, its synergetic linkages across the other operational domains, and the scale and scope of cyber effects requires an appreciation of the terms associated with cyber operations. The interpretation of terms can determine the structure of organisations, the types of capabilities acquired, the type of response to a situation, or who holds the responsibility for various functions. Wholesale labelling of the conduct of military activities in the cyber domain as cyber warfare is too simplistic and understates the breadth of cyber operations. This chapter establishes a clear picture of the hierarchal flow of

43 Source: Amit Sharma, 'Cyber wars: a paradigm shift from means to ends', Christian Czosseck & Kenneth Geers (eds), *Cryptology and Information Security Series – Volume 3 – The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Press, Amsterdam, 2009, Figure 1, p. 7.

cyber-related terms and provides insight into the scope of activities involved in the conduct of cyber operations. If the RAAF and the broader ADF organisation are to exploit cyberspace to its maximum potential, the adoption of standardised terminology and definitions must occur from the governmental executive down to the front-line warrior.

Environments

At the top of the definitional tree are the environments in which all actions occur. The environments are divided according to the aggregate of surrounding conditions. These conditions are characterised by vacuum, gas, liquid, solid and, with an awareness of cyberspace, ether.[44] All actions, military or otherwise, occur within or across the bounds of these environments. The first four physical environments have been evident for millennia; however, the fifth environment, which I refer to as ether, emerged with the development of computers, network structures, and the technology to transmit data between nodes. The physical environments can be clearly delineated by the presence of water, earth, air or, in the case of vacuum, the lack of physical elements. Ether is more difficult to visualise as it permeates all the other environments. Ether encompasses the collective digital memory systems, internets and intranets, software, hardware, and the electromagnetic spectrum and transmission lines of civilian, commercial, military and governmental organisations through which data traverses nearly instantaneously. While the concept of information will be dealt with separately, it is important to note that data is not information; rather a set of binary characters that, on their own, represent no coherent meaning.[45] Information is data that has been processed and interpreted in relation to a specific context. In 2010, US joint doctrine added a fifth environment to acknowledge the influence of cyberspace on the conduct of warfighting activities; it labelled this new environment, informational.

Joint Publication 3-0: *Joint Operations*, characterises environment in the operational context as 'the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander'.[46] Joint doctrine differentiates the physical areas—vacuum, gas, liquid and solid—from the ethereal environment, which it refers to as

---

44 Lieutenant Colonel Sebastian M Convertino II, Lou Anne DeMattei & Lieutenant Colonel Tammy M Knierim, *Flying and Fighting in Cyberspace*, Maxwell Paper No. 40, Air University Press, Maxwell Air Force Base, AL, 2007, adapted from Table 3, p. 10.

45 David S Alberts, John J Garstka, Richard E Hayes & David A Signori, *Understanding Information Age Warfare*, CCRP Publication Series, Washington, DC, 2001, p. 16.

46 United States Joint Chiefs of Staff, Joint Publication 3-0: *Joint Operations*, Joint Chiefs of Staff, Washington, DC, 2006 (incorporating Change 2, 22 March 2010), p. xvi.

informational. Joint Publication 3-0 offers the information environment as 'a global environment composed of all individuals, organizations, and systems that collect, process, disseminate, or act on information.'[47] While arguably information is an operational dimension (addressed later in this chapter) rather than an environment, the acknowledgement of an environment existing outside the physical realms formalised the long-held realisation of many that cyberspace was a warfighting domain.[48]

Domains

There is no US doctrinal or internationally agreed on definition for what delineates a domain. Patrick Allen and Dennis Gilbert posit that a domain is a 'sphere of interest and influence in which activities, functions, and operations are undertaken to accomplish missions and exercise control over an opponent in order to achieve desired effects.'[49] Domains require capabilities to have unique qualities to operate within them. They cannot fully encompass any other domain, and some degree of control must be possible within each sphere. Further, friendly and opposing capabilities must be capable of having a shared presence, but the opportunity will exist to gain synergy from other domains, and conduct asymmetric actions across domains.[50] Joint Publication 3-0 espouses four physical warfighting domains—air, land, maritime and space; and one informational domain—cyberspace.[51]

---

47 ibid., p. II-22.

48 Martin C Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, New York, NY, 2007, p. 2.

49 Patrick D Allen & Dennis P Gilbert Jr., 'The information sphere domain – increasing understanding and cooperation', Christian Czosseck & Kenneth Geers (eds), *Cryptology and Information Security Series – Volume 3 – The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Press, Amsterdam, 2009, p. 133.

50 ibid., p. 134.

51 United States Joint Chiefs of Staff, Joint Publication 3-0: *Joint Operations*, p. xvi.

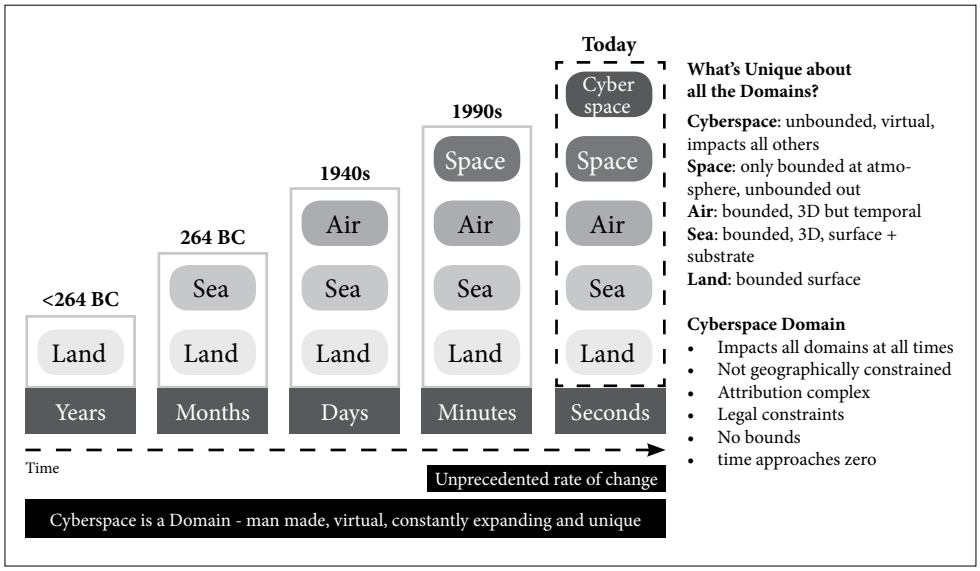

Figure 3–2: The accelerating calculus of war[52]

Figure 3–2 depicts the evolution of warfighting domains, with cyberspace firmly ensconced as a separate and unique domain. Each of these domains relate directly to the physical or ethereal environments.

The 2005 US *Capstone Concept for Joint Operations* broadened the idea of domains when it referred to them as 'any potential operating "space" through which the target system can be influenced--not only the domains of land, sea, air, and space, but also the virtual (information and cyber) and human (cognitive, moral, and social) domains'.[53] The *Capstone Concept for Joint Operations* documents provide the guiding principles for the development of joint doctrine. The 2005 *Capstone Concept* document planted the seed for the realisation of cyberspace as a separate domain. The 2009 *Capstone Concept for Joint Operations* firmly ensconced cyberspace as separate from the four physical domains, and linked future military success with the ability to successfully operate in cyberspace and integrate cyber capabilities with those capabilities resident in other domains.[54]

52 Source: Larry Burger, 'Cyberspace', US Army Space and Missile Defense Command, Future Warfare Center, Huntsville, AL, 2011, Slide 6.

53 United States Joint Chiefs of Staff, *Capstone Concept for Joint Operations*, Version 2.0, Joint Chiefs of Staff, Department of Defense, Washington, DC, 2005, p. 16.

54 United States Joint Chiefs of Staff, *Capstone Concept for Joint Operations*, Version 3.0, Joint Chiefs of Staff, Department of Defense, Washington, DC, 2009, p. 3.

The physical domains provide the warfighter dimensions in which to conduct operations; cyberspace provides an extra dimension to engage in conflict. Lieutenant General Robert J Elder, as Commander of Eighth Air Force, echoes this notion in his statement, 'Cyberspace exists alongside the other warfighting domains and should be protected and exploited in a similar fashion.'[55] However, labelling cyberspace as a domain is one thing, understanding what it is and what it encompasses is entirely another thing.

Cyberspace

There are almost as many definitions for cyberspace as there are academic books on the subject. This is not unexpected because cyberspace, as a warfighting domain, only emerged in the 1990s, with explicit cyber operations tracing back to Operation *Desert Storm*. In reality, cyber activities predate Operation *Desert Storm* with intelligence agencies using computer-based technologies during World War II; indeed the Internet was founded in the 1960s and flourished during the 1980s.[56]

However, it was not until the mid-1990s when net-centric warfare, hosted in cyberspace, began to emerge as a new form of warfare. This emergence, combined with growth in intelligence, surveillance and reconnaissance (ISR), triggered many academics and military scholars to posit that warfare was undergoing a revolution in military affairs.[57] Operation *Allied Force*, the 1999 NATO war against the Federal Republic of Yugoslavia, saw cyberspace crystallise as a warfighting domain with cyber operations used to support and shape the air campaign.[58] A clear understanding of what cyberspace is, and importantly what it is not, is critical to appreciating the effects cyber operations can produce. Following is an assortment of definitions available on cyberspace:

- *Joint Publication 1-02.* A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[59]

---

55 Lieutenant General Robert J Elder Jr., quoted in Henry S Kenyon, 'Cyberspace Command logs in', *SIGNAL Online,* August 2007, viewed 13 March 2011, <http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1362&zoneid=212>.

56 Rebecca Grant, *Rise of Cyber War*, Mitchell Institute Press, Washington, DC, 2008, p. 6.

57 David J Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, Cass Series: Strategy and History, Volume 9, Frank Cass, New York, NY, 2004, p. 49.

58 Grant, *Rise of Cyber War*, p. 6.

59 United States Joint Chiefs of Staff, Joint Publication 1-02: *Department of Defense Dictionary of Military and Associated Terms*, Joint Chiefs of Staff, Washington, DC, 2010, p. 92.

- *Joint Publication 3-0*. Cyberspace consists of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Within cyberspace, electronics and the electromagnetic spectrum are used to store, modify, and exchange data via networked systems.[60]
- *Martin Libicki*. Cyberspace is a replicable construct that is built rather than born. It can exist in multiple locations simultaneously; in cyberspace, no single *there* exists. Cyberspace has three layers: physical hardware; the syntactic level where data and information are constructed and controlled; and the semantic layer that contains the information meaningful to the end user, whether it be human or machine.[61]
- *Dorothy Denning*. Cyberspace is the information space consisting of the sum total of all computer networks. Information space is defined as the aggregate of all information services available to an entity, such as printed documents, computers, communication systems, and all the information present in an organisation's physical and cognitive environment.[62]
- *The US National Strategy to Defend Cyberspace*. Cyberspace is the nervous system of public and private institutions—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fibre-optic cables that make our critical infrastructures work.
- *National Military Strategy for Cyber Operations*. 'An operational domain whose distinctive and unique character is formed by the use of electronics and the electromagnetic spectrum to create, modify, exchange, and exploit information via connected and internetted information systems and their associated infrastructures.'[63]

Definition. From these definitions, cyberspace can be characterised as a domain that exists in both the physical and cognitive dimensions, encompasses a networked system of computers, supported by a communications infrastructure, and within which information shifts between actors. Rebecca Grant asserts that

---

60 United States Joint Chiefs of Staff, Joint Publication 3-0: *Joint Operations*, p. II-22.

61 Libicki, *Conquest in Cyberspace*, pp. 5–8.

62 Dorothy E Denning, *Information Warfare and Security*, ACM Press, New York, NY, 1999, p. 22.

63 Daniel T Kuehl, 'From cyberspace to cyberpower: defining the problem', Franklin D Kramer, Stuart H Starr & Larry Wentz (eds), *Cyberpower and National Security*, National Defense University Press and Potomac Books, Washington, DC, 2009, p. 48. This definition was adapted from *The National Military Strategy for Cyberspace Operations*, 2006, p. ix.

early definitions of cyberspace were too focused on the electromagnetic (EM) spectrum, which led to debates about whether technologies such as the telegraph were *cyber-like*.[64] The EM spectrum is an important element of cyberspace. It provides the manoeuvre space for cyber operations, but it is not the basis of the domain. Information, and its exchange between users, provides meaning to this sphere of influence. The physical elements of cyberspace provide the essential framework in which its cognitive element, information, is created, modified, stored and transmitted. The challenge to warfighters is to take a definition that combines the physical and cognitive realms, and develop a framework within which to carry out combat operations.

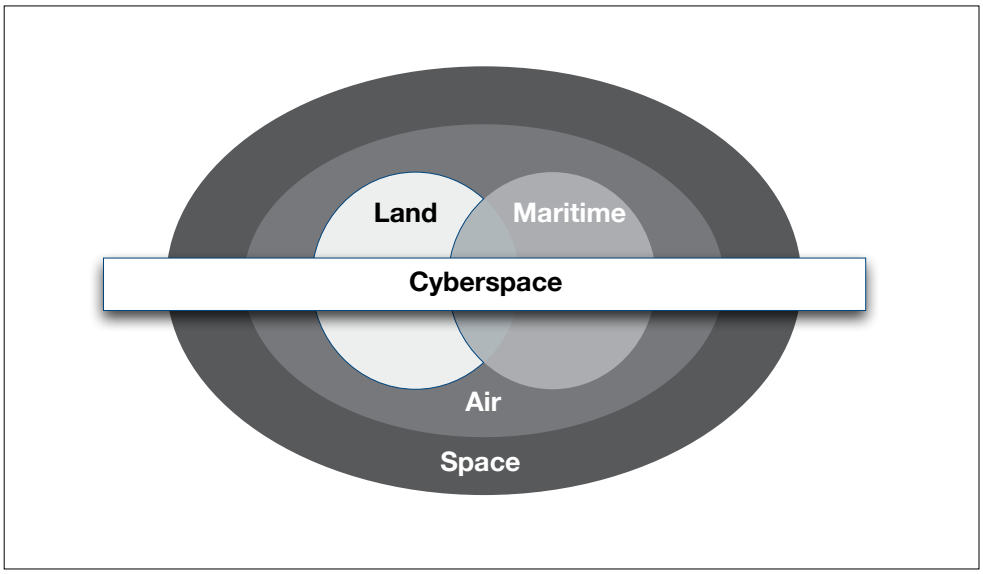

Figure 3–3: Warfighting operational domain relationships[65]

The concept of cyberspace is difficult to visualise. Land, sea, air, and even space are regions that have a physical presence; however, as depicted in Figure 3–3, cyberspace pervades them all. Soldiers, sailors, pilots and astronauts can interact directly with these environments. Cyberspace is a phenomenon where human connection is on the peripheral. Software is the proxy the warfighter uses within the domain to substitute for a physical presence. If cyberspace was the human

64 Grant, *Rise of Cyber War*, p. 7.

65 Source: United States Air Force, Air Force Doctrine Document 3-12: *Cyberspace Operations*, Department of the Air Force, Washington, DC, 2010, p. 20.

body, servers, cables and supporting infrastructure would be physiological. In cyberspace, computers are analogous to the brain, networks to synapses, data to the action potentials, and information to thought.[66] Man-made technology allows humans to enter and exploit the air, space and maritime warfighting domains. Humans access the air domain using technology to carry payloads over distances to cause effects. Similarly, it takes technology to access the cyber domain to carry software payloads over distances to cause effects. However, though humans cannot physically enter the cyber domain, technology remains the lever to exploit warfighting advantages.[67] Over the last decade, the military has steadily built a better picture of cyberspace, expanding its understanding of information effects within the domain, as well as the enabling power information provides to capabilities across other domains.

Information

Information is the core around which command, control and execution of military operations occur. Every event in life revolves around the creation, manipulation, transmission and application of information. At its basics, information is the consequence of putting individual observations into some significant context.[68] These observations could be from sensors, human or machine, or from the collection of data items. Data is the depiction of individual facts, concepts or directions that are capable of transmission, processing and interpretation by man or machine.[69] Information is blind; it does not reflect truth, merely a translation of the received data. As Edward Mann states, 'information is passive and always exists … whether anyone pays attention to it or not … it can be collected, collated, analyzed, "fused", packaged, disseminated, and even managed.'[70] Data can be incorrectly created through misinterpretation of an observation or entry error, manipulated by a third party, or corrupted during transmission. The information extracted from data is merely a representation of what is received. Knowledge is drawn from conclusions, deduced from patterns, and gleaned from information.

---

66 The brain's cerebral cortex contains roughly one billion synapses. These neurons communicate with one another by means of long protoplasmic fibres called axons. Axons carry trains of signal pulses called action potentials to distant parts of the brain or body and target them to specific recipient cells.

67 Kuehl, 'From cyberspace to cyberpower', p. 29.

68 Alberts et al., *Understanding Information Age Warfare*, p. 16.

69 ibid., p. 17.

70 Colonel Edward C Mann III, USAF, *Thunder and Lightning: Desert Storm and the Airpower Debates*, Air University Press, Maxwell Air Force Base, AL, 1995, p. 152.

Knowledge. Unlike information, knowledge is active. It cannot sit in a filing cabinet or be stored on a hard drive. It must be applied to a context to be relevant and useful to the decision-maker. The location of an aircraft is information; it only becomes knowledge when the location is linked to a context and an operational environment.[71] The combination of knowledge, experience and context provides understanding to information sufficient to predict consequences of actions and develop awareness of situations.[72] Edward Waltz espouses that this combination is termed wisdom, and, as depicted in Figure 3–4, it is at this level of the information hierarchy that decision-making occurs.[73] All actions from the tactical to strategic levels require decision-making. Thus, decision-making is the fundamental component in the command, control and execution of military actions.

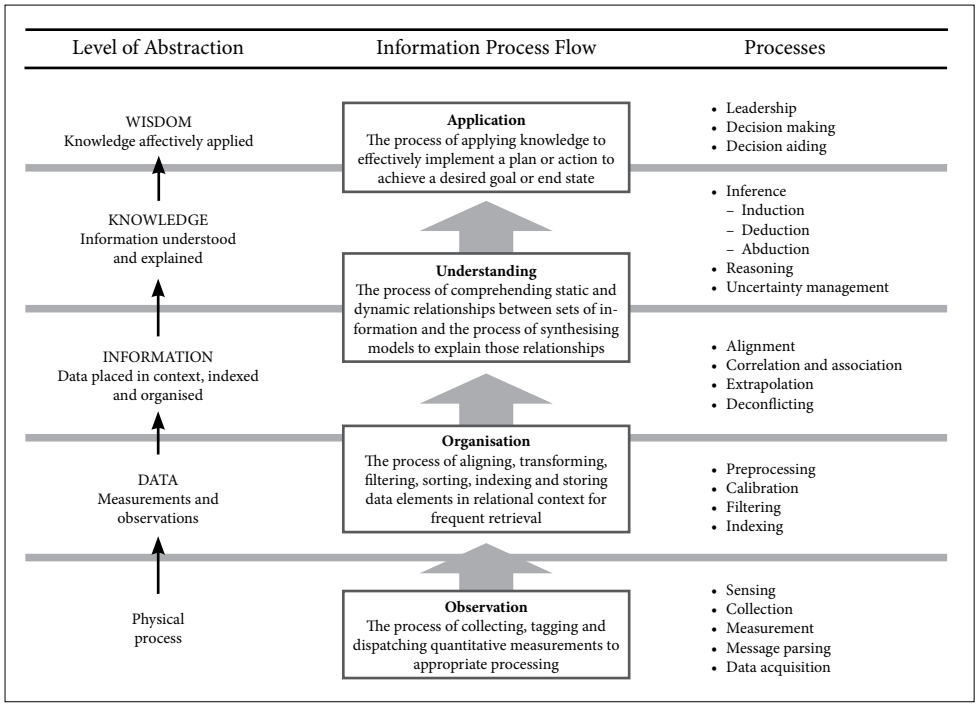

Figure 3–4: Information hierarchy[74]

71 ibid., p. 153.

72 Alberts et al., *Understanding Information Age Warfare*, pp. 16–20.

73 Waltz, *Information Warfare*, pp. 50–51.

74 ibid., p. 51, Figure 2.1.

Cyberspace is not the sole repository of information, but it is becoming the most prevalent medium and thus critical to military operations. Hardcopy books, photographs and recordings are examples of non-cyber based information, though increasingly these media are reproduced in cyberspace. The 2011 *National Military Strategy* acknowledged the pervasiveness of this domain when it stated, 'cyberspace capabilities enable Combatant Commanders to operate effectively across all domains'.[75] Dependence breeds vulnerabilities and the US, along with most other nations, is becoming increasingly reliant on the cyberspace domain for enabling many national security requirements.[76] This reliance opens the door for the cyber warrior to exploit the cyberspace domain through cyber attack, but places even greater importance on cyber defence to maintain any asymmetric advantages across all the warfighting domains.

Information Operations

Information is an essential element of military operations, but as information and cyber share a synergy rather than an identity, the role of information operations differs from cyber operations. Cyber is one medium through which information operations, such as directed psychological operations, are conducted.[77] As Rebecca Grant states, 'information operations and cyber operations are closely related, but they aren't the same thing'.[78] As described in Joint Publication 3-13: *Information Operations*, information is used 'to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own'.[79] Information operations, in some form, have been around for thousands of years. Sun Tzu is perhaps the earliest recorded advocate of using information as a tool of war, asserting 'All warfare is based on deception' and all deception

---

75 United States Joint Chiefs of Staff., *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership*, Joint Chiefs of Staff, Washington, DC, 2011, p. 10.

76 President of the United States, *National Security Strategy – 2010*, Executive Office of the President, Washington, DC, 2010, p. 8.

77 Richard Mesic, Myron Hura, Martin C Libicki, Anthony M Packard & Lynn M Scott, *Air Force Cyber Command (Provisional) Decision Support*, RAND Project Air Force, RAND Corporation, Santa Monica, CA, 2010, p. 13.

78 Grant, *Rise of Cyber War*, p. 7.

79 United States Joint Chiefs of Staff, Joint Publication 3-13*: Information Operations*, Joint Chiefs of Staff, Washington, DC, 2006, p. ix.

should lead to confusion.[80] Taken literally, this is fully correct; an alternative interpretation could be that all war is based on influence, with information and deception at its core.

Information operations work! Information operations seek to influence the decision-making process of the opposing commander because, as Clausewitz and Sun Tzu assert, the commander is the decisive factor—a centre of gravity.[81] In World War II, the Allies manipulated information in the lead-up to Operational *Overlord*, to convince the German decision-makers that the invasion of Europe was to occur in a location other than Normandy. Operation *Fortitude* was a major information operation, involving the controlled leakage of falsified information, to mislead German High Command into thinking Norway and Calais was the invasion site. *Fortitude* used wireless traffic to deceive German commanders into believing General Patton's fantasy 1st Army Group was real and a threat.[82] More recently, Operation *Desert Storm* invoked electronic warfare from the outset to deceive Iraqi controllers into thinking that large packages of aircraft were inbound to Baghdad when no such formations existed.[83] While the delivery platforms were electronic, the weapon was information, and the target was Iraqi decision-makers. As technology progresses and cyberspace opens up to military activities, information operations functions increasingly occur in the cyberspace domain.

Information Environment

Common in much of the literature on information operations is a linkage to the information environment.[84] Joint Publication 3-13 states the information environment represents the 'aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information'.[85] It is within this environment that decision-making occurs in a way best immortalised by Colonel John Boyd's observe, orient, decide and act (OODA) loop. Boyd argued

---

80 Sun Tzu & Samuel B Griffith, *The Illustrated Art of War*, Oxford University Press, New York, NY, 2005, pp. 78 and 96.

81 ibid., p. 121.

82 Max Hastings, *Overlord: D-Day and the Battle for Normandy*, 1st Vintage Books edition, Vintage Books, New York, NY, 2006, pp. 63–65.

83 Williamson Murray & Major General Robert H Scales, Jr., *The Iraq War: A Military History*, Belknap Press of Harvard University Press, Cambridge, MA, 2003, pp. 2–3.

84 The terms *information domain* and *information warfare model* represent the same concept as the term *information environment*, and share three common components: physical, information and cognitive/perceptual.

85 United States Joint Chiefs of Staff, Joint Publication 3-13: *Information Operations*, p. x.

that the key to success in combat was to have a more effective OODA loop than the adversary. This is achieved by having better information processes, but also by disrupting the effectiveness of the adversary's OODA loop.[86] Information operations seek to exploit opportunities on the observe and orient elements to disrupt or corrupt the adversaries' decision-making processes and reduce the effectiveness of their actions.

There are numerous methods to analyse the conduct of operations against information systems. Martin Libicki views information systems in terms of three physical, synaptic, and semantic layers. The physical layer consists of the various means that permit the circulation of informational bits. The means can be computers, routers, satellites, or cables, with circulation varying from radio frequency energy to electrical signals and photons. The physical later is vulnerable to attack by direct damage to the hardware or interception of the information as it circulates across the system.[87] The syntactic layer consists of the instructions that tell information systems what to do with bits that are being circulated through the physical system. In modern computers, the syntax is the operating system and associated applications, while on networks it is the Internet protocols. It is in this layer where hackers operate, inserting malware to corrupt or damage the information systems processes. Syntax determines where information packets are stored and how they are processed.[88] The semantic layer provides meaning to the information content. For this reason, it is at the semantic level where deception operations against people and logic processing systems occur.[89] Other authors, such as Chris Scott, consider how information operations occur within the three interrelated dimensions of physical, informational (cyber) and cognitive domains, as indicated in Figure 3–5.

---

86 Grant T Hammond, *The Mind of War: John Boyd and American Security*, Smithsonian Institution Press, Washington, DC, 2001, pp. 189–91.

87 Libicki, *Conquest in Cyberspace*, p. 24.

88 ibid., pp. 24–25.

89 ibid., p. 25.

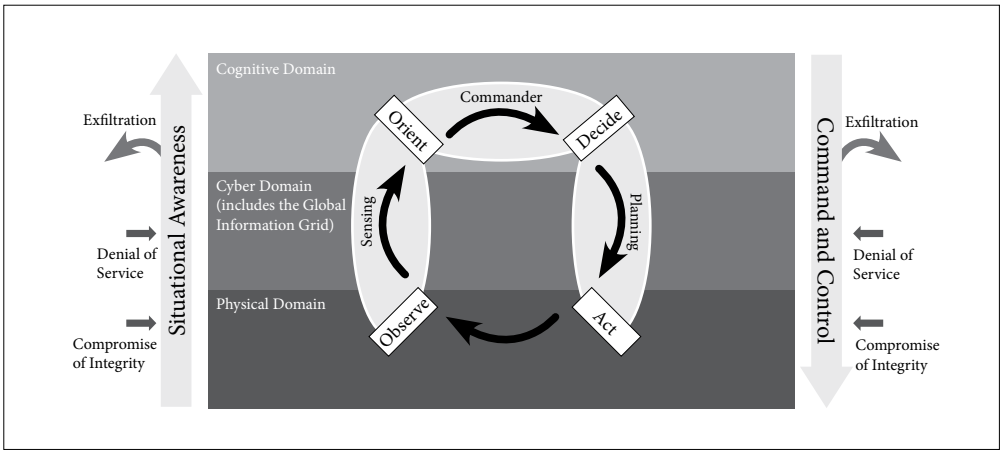

Figure 3–5. The information dimensions and their role in decision-making[90]

Dimensions

The physical dimension contains all the hardware and associated infrastructure required to conduct information operations. It includes the communication capabilities that reside in all the warfighting domains. With advancements in technology, a greater emphasis is placed on the physical capabilities that reside in cyberspace, such as computers, servers, wireless systems and cables that support the transmission of data.[91] The informational dimension is where information is collected, processed, stored, disseminated, displayed and protected.[92] Examples of information include air tasking orders, propaganda leaflets, maps, publications and television broadcasts. This dimension is about the content and flow of information rather than the medium used to produce the information. The third dimension, cognitive, is where information is translated into knowledge for use in the decision-making process, as depicted in Figure 3–5. As Clausewitz argues, it is the mind of the commander where genius occurs and therefore the key to success

90 Source: Chris Scott, 'Cyber Warfare: A Perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace', presentation at US Army Cyber Symposium, September 2008, Information and Systems Technology Group, MIT Lincoln Laboratory, Lincoln, MA, 2008, Slide 7 of 28.

91 United States Joint Chiefs of Staff, Joint Publication 3-13: *Information Operations*, p. I-1.

92 ibid., p. I-2.

in war lies within this dimension.[93] Joint Publication 3-13 emphasises 'this is the dimension in which people think, perceive, visualize, and decide.'[94]

Information conveyed from the physical and information dimensions, such as commander's intent, training instructions or propaganda, is translated into meaning by associated factors such as: 'leadership, morale, unit cohesion, emotion, state of mind, level of training, experience, situational awareness, as well as public opinion, perceptions, media, public information, and rumors.'[95] The functions of information operations take place within these dimensions and across all the warfighting domains, though more functions are utilising cyberspace as technology provides greater opportunities.

Information operations encompass a broad scope of functions, and numerous books are available on the subject. However, to appreciate the differences between information and cyber operations, Timothy Thomas in his book, *Cyber Silhouettes*, offers a definition that captures many of the information concepts across much of the literature. He posits:

> An IO [information operation] is a number of technical, influence, and effects-causing operations (plus their countercapabilities) used from peacetime to postconflict scenarios to achieve a stated goal via means of destruction, persuasion, protection, control, or neutralization. These activities are aimed at the decision-making of leaders, combatants, and the general populace, and include all means to gather and distribute information.[96]

Complexity. Though this definition may seem overly proscriptive, it does portray the complexity of information operations. A common problem in describing information operations is that the functions are so broad that information, as Leigh Armistead posits, 'is at once everything, and it is nothing'.[97] In many ways, the evolution of information operations was a catch-all for capabilities that did not seem to fit anywhere else. As information was primarily a responsibility of the intelligence community, a number of associated intelligence capabilities were clustered under the information operations umbrella. Joint Publication 3-13: *Information Operations* assists in reducing some of this complexity by breaking

---

93 Carl von Clausewitz, Michael Eliot Howard & Peter Paret, *On War*, rev. ed., Princeton University Press, Princeton, NJ, 1984, p. 100.

94 United States Joint Chiefs of Staff, Joint Publication 3-13: *Information Operations*, p. I-2.

95 ibid., p. I-2.

96 Timothy L Thomas, *Cyber Silhouettes: Shadows Over Information Operations*, Foreign Military Studies Office (FMSO), Fort Leavenworth, KS, 2005, p. 25.

97 Leigh Armistead (ed.), *Information Operations: Warfare and the Hard Reality of Soft Power*, 1st edition, Brassey's Issues in Twenty-First Century Warfare, Brassey's, Washington, DC, 2004, p. 19.

the functions into core, supporting and related capabilities. Core capabilities are those required for the planning and execution of operations in the information environment. Supporting capabilities have military purposes other than information operations but either operate in the information environment or have impact on the information environment. The third group of related capabilities interfaces with core and supporting capabilities, but have separate and distinct purposes.[98] The capabilities within each group are:

- *Core capabilities*: Electronic warfare, operations security, psychological operations, military deception, and computer network operations.
- *Supporting information operation capabilities*: Information assurance, physical security, physical attack, counterintelligence, and combat camera.
- *Related information operation capabilities*: public affairs, civil-military operations, and defence support to public diplomacy.

Core Capabilities[99]

Electronic warfare (EW) means many things to many people; however, doctrinally, EW encompasses any military use of the electromagnetic spectrum to influence an enemy either directly or indirectly and consists of Electronic Attack, Electronic Protection and EW Support. Cyberspace and EW can share similar portions of the electromagnetic spectrum, but their relationship is symbiotic, with capabilities within cyberspace supporting the conduct of EW.

1. *Electronic Attack* utilises the electromagnetic spectrum to actively or passively degrade or destroy an adversary's military capability.
2. *Electronic Protection* seeks to minimise the effects of electronic warfare on friendly capability, from either electronic fratricide or an adversary's electronic attack.
3. *Electronic Warfare Support* builds situational awareness of an adversary's use of the electromagnetic spectrum for threat avoidance, targeting and intelligence.

Operations Security (OPSEC) identifies friendly information requiring security from the enemy's collection efforts such that the enemy cannot determine friendly intentions. Because cyberspace is so pervasive, a cyber OPSEC plan is critical.

---

98 United States Joint Chiefs of Staff, Joint Publication 3-13: *Information Operations*, p. I-6.

99 ibid., pp. II-1 – II-5.

Psychological Operations seek to influence a target audience with the use of selected truthful information in order to coerce this audience to accept a position advantageous to friendly objectives. Television, radio and social media hosted in cyberspace are common mediums.

Military Deception seeks to influence an adversary's information process such that the friendly operational intentions are misinterpreted or masked. As cyberspace hosts many adversaries' information processes, cyber operations will play a significant role in this function.

Computer network operations (CNO) are actions undertaken by military forces in cyberspace that target an adversary's information systems, defend Department of Defence information systems, and focus on vulnerabilities in the adversary's systems to gather data on their capabilities and intentions. Because CNO is where the cyber rubber hits the information operations highway, this function is discussed in depth later in the chapter.

Supporting Capabilities[100]

Information assurance (IA) seeks to maintain the validity of information systems and trust in the information by ensuring the availability, integrity, authentication, confidentiality and non-repudiation of information. IA is a huge challenge for cyber operations but vital to the conduct of effective command and control. Conversely, cyber operations can downgrade an adversary's IA, corrupting their decision-making process.

Physical Security safeguards personnel, hardware and facilities from potential enemy actions including espionage, sabotage, damage or theft linked to information operations.

Physical Attack is the kinetic effects applied to the adversary's information systems, which in turn may influence target audiences.

Counterintelligence gathers information from intelligence sources in order to protect friendly forces from espionage and other intelligence activities. Cyber operations play an increasing role in the support of counterintelligence.

Combat Camera provides imagery to friendly forces in support of planning and operations across the spectrum of military missions. Most images are stored, disseminated and viewed through cyber capabilities.

---

100 ibid., pp. II-5 – II-8.

Related capabilities[101]

Public Affairs inform target audiences on the conduct of the operations. The Internet enables the rapid distribution of information to local and dispersed target audiences.

Civil-Military Operations are activities between the military, the civil population, or other government organisations that provide support to the civil community.

Defence Support to Public Diplomacy broadens awareness of international audiences to the foreign policies of a nation's government. The Internet facilitates the communication of the commander's strategic message to the global community

Cyber Network Operations

In Cyber Network Operations, the line blurs between cyber operations and information operations. Though, organisationally, the function can be listed under either, academic and doctrine writers argue that CNO belongs under one or the other. To avoid fratricide, duplication of effort, and turf wars between Services and agencies, an unambiguous national directive should delineate organisational responsibilities. The 2006 US *National Military Strategy for Cyberspace Operations* provides an excellent framework to develop responsibilities and operational objectives. The *National Military Strategy for Cyberspace Operations* lists three components of CNO: computer network attack, computer network defence, and computer network exploitation.[102]

Computer network attack (CNA) encompasses military 'operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.'[103] The term 'computer network attack' is becoming increasing redundant. Though CNA refers to a military operation, 'cyber attack' is becoming more accepted to describe activity by an individual, organisation, military or state that disrupts, denies, degrades, destroys or manipulates another party's cyber-based information. CNA supports military or national objectives, whereas cyber attack includes all motivations such as criminal, personal, financial, malicious, terrorism or political, as well as military. The US military operates under stringent regulations for the conduct of

101 ibid., pp. II-8 – II-10.

102 United States Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, redacted edition, Joint Chiefs of Staff, Washington, DC, 2006, p. GL-1.

103 ibid.

CNA. General Keith Alexander, Commander US Cyber Command, stated in his Senate confirmation hearing that offensive operations are conducted only after the issuance of an execute order and then in accordance with rules of engagement.[104] Offensive operations could include disabling the cyber elements of the adversary's command-and-control system or altering software code to corrupt sensor data. In many ways, CNA mirrors the targeting practices of kinetic operations.[105] Target selection is based on the target's perceived impact on lines of operation and its collective ability to erode the adversary's centre of gravity. The differences between the types of operations are the weapons, spread of execution, global reach, and attribution footprint.

Cyber weapons. The weapons of cyber attack are increasing in complexity as the technology behind information systems increases and the experience in this type of weapon design advances. This complexity is apparent in the new generation of weapons that adapt to the specific targeted system 'post launch', replacing the older generic viruses and worms.[106] Adaptive weapons are capable of self-replicating and modifying themselves to navigate through various levels of defence mechanisms.[107] The payload of these cyber weapons can lay dormant for years waiting for a remote trigger or for a set of conditions, such as a specific radar return or electromagnetic signature. The most common types of cyber weapons are manipulative software, termed malware worms, and distributed denial of service software.

Malware. The more relevant types of malware used in cyber attacks include viruses, worms and Trojan horses. The virus is a program that infects computers by attaching itself to a host program, then replicating itself and jumping across to another host. Like their biological namesakes, computer viruses spread through contact. Infected programs can be web-based (e.g. email attachments or websites) or attached to data or programs on a thumb drive or compact disc. Worms are self-propagating code that can automatically distribute themselves through network connections. Current generation worms can selectively infect targeted programs as they move through a network, making it difficult to trace origins. Trojan horses, as the name suggests, are programs concealed in software that appears benign, and will remain dormant until triggered by an outside command,

---

104 United States Senate, Committtee on Armed Services, 'Nomination of LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/Commander, US Cyber Command', US Senate, Committtee on Armed Services, Washington, DC, 2010, p. 11.

105 Sean Watts, 'Combatant status and computer network attack', *Virginia Journal of International Law*, vol. 50, no. 2, 2010, p. 399.

106 ibid., p. 402.

107 Gary Waters, Desmond Ball & Ian Dudgeon, *Australia and Cyber-Warfare*, Canberra Papers on Strategy and Defence, no. 168, ANU E Press, Canberra, 2008, p. 44.

a set of conditions, or a time limit. Trojan horses are data-collection tools, with keyloggers that report on key strokes to another system allowing monitoring of passwords and activities, as well as rootkits that allow the conduct of unauthorised logins and activities on a host system without the host's awareness.[108]

Distributed denial of service. This form of cyber attack seeks to make a target information system unavailable to intended users by flooding bandwidth or servers with emails or website-access requests.[109] The sheer volume of traffic, which can measure in the millions of hits per second, overwhelms servers causing them to crash, or clogs the bandwidth, restricting access to the targeted system and potentially other systems sharing the network.[110] Central to this form of cyber attack are the use of bots, which is software that accesses an individual computer, usually through malware, then surreptitiously sends out emails or pings targeted information systems.[111] The owner of the individual computer is normally oblivious to the cyber activity. When malware impregnates other computers, the bots can form a network allowing a distributed and coordinated attack on information systems. Depending of the proliferation of the network of bots, called botnets, millions of computers could be enslaved and participate in cyber attacks. This form of cyber attack perpetuates the dilemma faced by responders.[112] If the source of an attack is traceable, should the owners of the computers used in the attack be liable for retribution? How can an organisation responding to an attack guarantee attribution before initiating a counterattack? This form of attack could also shift the blame from the originator to a competitor—whether that is another organisation, another country or a neutral third party—or make the attack appear to originate internally to a targeted state.

Lieutenant General Alexander, in his Senate confirmation hearing for Commander US Cyber Command, stated that the issue of attribution would vex decision-makers who seek action and blame for a major attack. He acknowledged that the US Department of Defence is probed hundreds of thousands of times a day by attacker attempting to exploit the military information systems. Some are coordinated attacks, some seek out vulnerabilities in the system for use later, while

---

108 Horst K Saalbach, *Cyber War: Methods and Practice – Version 3.0*, Universität Osnabrück, Osnabrück, 2011, p. 9.

109 ibid., p. 10.

110 Richard A Clarke & Robert K Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st edition, Ecco, New York, NY, 2010, p. 25.

111 Japanese Ministry of Internal Affairs and Communications, 'What Is Bot?', viewed 18 May 2011, <https://www.ccc.go.jp/en_bot/>.

112 Saalbach *Cyber War Methods and Practice – Version 3.0*, p. 10.

others attempt to steal controlled information.[113] Cyber attacks are increasing and if the US, along with other nations, is to maintain the use of cyberspace, current defensive measures will require continual oversight and upgrades.

Computer network defence (CND) are 'actions taken through the use of computer networks to protect, monitor, analyze, detect and respond to unauthorized activity within Department of Defense information systems and computer networks'.[114] The US and other modern nations like Australia rely heavily on cyberspace-enabled activities to maintain their relative strategic advantages across all facets of their military capabilities. Continued access to cyberspace and protection of information systems from state and non-state actors seeking to counter our advantages is essential to the maintenance of our national interests. The cyber attacks on Georgia and Estonia brought home the vulnerability of military, government and civil-sector cyber-enabled capabilities from a targeted assault. Computer network defence is the function that seeks to protect military information systems from attack and ensure cyber-enabled capabilities can operate relatively unhindered in a contested cyber environment. Defence-in-depth is not as simple as putting up a firewall and sitting back to watch the viruses and Trojan horses being repelled. The complexity and ubiquity of cyberspace encourages a potential attacker to continually probe for vulnerabilities in a system that relies on friendly information to travel back and forth through any defences with minimal impact. Unfortunately, the layers of defence are not always successful.

Even the best are vulnerable. The US has not always been successful in defending its network. The Department of Defense operates more than 15 000 networks, seven million computing devices, and employs more than 90 000 personnel involved directly in information systems.[115] The challenge of securing an information system this extensive almost guarantees the system will have vulnerabilities.

Deputy Secretary Lynn indicated that Department of Defense suffered its worst cyber attack in 2008 when a single thumb drive, containing malware from an unidentified foreign agency, was inserted into a US network. The malware was a combination of worm and Trojan horse programs, silently spreading like a virus across every system touched. It then exported data from those systems to foreign

---

113 United States Senate, Committee on Armed Services, 'Nomination of LTG Keith B. Alexander, USA, to Be General and Director, National Security Agency/Commander, US Cyber Command', pp. 17–18.

114 United States Joint Chiefs of Staff, Joint Publication 3-13: *Information Operations*, p. GL-5.

115 Deputy Secretary of Defense William J Lynn, 'Remarks on Cyber at the Council on Foreign Relations', Council on Foreign Relations, New York City, NY, 2010, viewed 20 March 2011, <http://www.defense.gov/speeches/speech.aspx?speechid=1509>.

organisations virtually unnoticed. Widespread use of thumb drives enabled the penetration of classified and unclassified systems. [116] The US changed its security protocols, but the character of the attack made analysing the degree of damage difficult. The event pushed the issue of cyber defence to the forefront of many in the military who may have considered the US system secure. Reality touched the Department of Defense, and cyber defence is now taken more seriously by a wider audience. Unfortunately, like most other revelations, it took a crisis to be the catalyst for change.

Attribution. If a cyber attack calls for a response, whom do you target? Deputy Secretary Lynn highlighted that data from a keystroke can travel around the world in less than 150 milliseconds, but identifying the perpetrator of an attack can take months.[117] If sufficiently advanced states or organisations can shield their identity or deflect blame to another party, is there a place for deterrence in cyber operations? Equally, what if the attacker had very little reliance on cyberspace, such as North Korea or a terrorist group; how effective would a cyber response be?

In these situations, it is apparent that in developing a deterrence strategy against cyber attack, offensive cyber operations play only a small part in potential responses. Cyber attack can be the cheapest form of offence an adversary can develop. A team of less than 100 military or state-sponsored information technology specialists can develop tools that pose a serious threat to the opposition's physical capabilities. The threat may not be direct, though that may not be too far off. But information on an aircraft's radar, a ship's defensive systems, or a tank's firepower capabilities can identify weaknesses that the adversary can exploit—all with the operators unaware that their strengths have been compromised.[118]

Deterrence. Any state that relies on cyberspace for its national interests has a stake in dissuading potential attackers from executing their offensive plans. As Martin Libicki states, 'Deterrence is in the mind of the potential attacker', therefore deterrence is measured by the resolve of the adversary, which is almost impossible to gauge in the ubiquity of cyberspace. [119] Cyber weapons are not nuclear weapons; they are not existential threats. A cyber attack can seriously degrade a military's capabilities or affect the lifestyle of a nation, as per Estonia in 2007 and Georgia in 2008, but cyber by itself does not threaten the survivability of a country. Building

116 ibid.

117 ibid.

118 ibid.

119 Martin C Libicki, *Cyberdeterrence and Cyberwar*, RAND Project Air Force, RAND Corporation, Santa Monica, CA, 2009, p. 183.

a bigger or better 'cyber bomb' is not likely to have the same deterrent influence in cyber as atomic weapons had on nuclear deterrence. Libicki argues, 'the better one's defenses, the less likely it is that an attack will succeed and so the less often a cyber deterrence policy will be tested' and 'a good defense adds credibility to the threat to retaliate' and 'good defenses have a way of filtering out third-party attacks'.[120] If two walls confront an attacker, one made of thick steel and one made of aluminium, and his weapon is a metal spike, it is likely he will attack the weaker structure, unless he is focused on the steel target; even then, he is unlikely to succeed.

Therefore, deterrence in cyberspace should include both strengthened defences and the threat of retaliation. The more robust an organisation's cyber defence, the less risk of a cyber attack occurring because the attacker may assess the futility of his plan. Similarly, the more robust the defences, the lower the risk that a cyber intrusion will succeed. But a cyber attack is an attack against the state, whether it exceeds a political threshold for initiating a national response or not. Therefore, as with any deterrent effort, strategy will be more effective if it draws on all the elements of national power. Cyber is just one tool in the deterrence quiver.[121]

Computer network exploitation (CNE) is activities that enable 'operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks'.[122] From a broad view, the actions undertaken to conduct computer network attack and computer network exploitation can appear very similar.[123] The two functions may focus on the same information systems and use similar technologies to undertake their operations. The difference between the two boils down to purpose. In computer network attack, cyberspace provides the opportunity to influence an adversary's decision-making ability, whereas those conducting computer network exploitation use cyberspace to support their own decision-making ability. Information, such as operational plans, platform capabilities, intelligence assessments, logistical status, and personnel data, is exported from the adversary's information systems to develop a better knowledge base on the enemy's capabilities and intent. The importance of this type of information has been acknowledged for thousands of years. Sun Tzu espoused that intelligence and secret operations are essential to an army's success in war;

---

120 ibid., p. 73.

121 Richard L Kugler, 'Deterrence of cyber attacks', Franklin D Kramer, Stuart H Starr & Larry K Wentz (eds), *Cyberpower and National Security*, National Defense University Press and Potomac Books, Washington, DC, 2009, p. 310.

122 United States Joint Chiefs of Staff, Joint Publication 3-13: *Information Operations*, p. GL-6.

123 Mesic et al., *Air Force Cyber Command (Provisional) Decision Support*, p. 9.

'upon them the army relies to make its every move'.[124] For Sun Tzu, intelligence came from agents or spies; in computer network exploitation the Trojan horse malware inserted to siphon off information represents cyber agents, performing the same function and still as critical to success in war.

Access is the gateway to cyber operations. Access is an element of cyber operations common to all countries. In cyber operations access is everything. It is the gate through which all cyber weapons travel to achieve their effects. If access is denied, as is the goal of cyber network defence, offensive cyber operations are muted. The military have a prime role in establishing and maintaining cyber access, though in cyber terms the period for access can be measured in seconds. Access is accomplished in three ways. First, through remote access; this is the admission into and out of a targeted system from home station system. For all military operations, the Defence Signals Directorate (DSD) in Australia and the Government Communications Headquarters (GCHQ) in the UK conduct these actions. A second type is close access where the military units operate close enough to conduct electromagnetic (EM) or electronic surveys of the local information systems. Military units could scan or map the local EM environment for uses such as cell phones, Wi-Fi transmitters, or any use of the EM spectrum in a local area. This task could be conducted by any trained ground unit, or by air platforms equipped with appropriate sensors. This is an example of conducting cyber operations across the EM spectrum. The third type is closed access and is likely to sit in the realm of Special Forces units. Closed access is where specialists physically break into a building, put hardware and software onto a closed loop information system, capture and send information out to a receiver, and rebroadcast the data to another location.

Cyber warfare = cyber attack + defence. Clausewitz asserts that the defensive form of warfare is stronger than offence, but it has a negative purpose and should be the primary function only as long as weakness compels. However, attack has the positive purpose of conquest and, if conflict is unavoidable, increases the capacity to wage war.[125] Thus, Australia has placed a large emphasis on security because Australia's preferred approach is to use actions other than the use of force. Robust cyber defence provides two major advantages: it provides Australia the ability to minimise the disruption or damage from cyber attack, regardless of the perpetrator; and supports the exploitation of cyberspace by friendly offensive forces, both kinetic and non-kinetic. Australia's cyber attack capabilities, like those of most other nations, are classified. However, the Defence White Paper 2009 indicated that Australia is undertaking a major enhancement of Defence's cyber

124 Sun Tzu & Griffith, *The Illustrated Art of War*, p. 239.

125 Clausewitz, Howard & Paret, *On War*, p. 358.

warfare capability to provide, amongst other capabilities, 'a much-enhanced cyber situational awareness and incident response capability'.[126]

As previously argued, cyber warfare includes both offence and defence. Similar types of cyber weapons used to attack friendly information systems are available for use during the conduct of cyber-attack operations by Australian cyber forces. As with kinetic operations, Defence will be restricted in target selection, with an authorisation to execute dependent upon the degree of collateral damage, the effects generated by the attack, and the subsequent second and third-order consequences. Unlike kinetic effects, many of these effects are difficult to accurately predict, even with precision cyber targeting. Cyber-attack operations will produce measurable strategic, operational and tactical effects because information influences decision-making.

But information by itself will not win a war. Therefore, cyber attack, and more broadly cyber warfare, is unlikely to be used in isolation from the other elements of war. Defence will use cyber operations during all phases of a conflict, and these could make up a large percentage of the shaping operations to reduce the physical footprint in theatre. During the more active phases, cyber operations will be conducted to support air, sea, land and space activities, and may be used to support the diplomatic, economic and informational instruments of national power. Defence continues to expand its cyber operations to enhance it capabilities across all the warfighting domains. Cyberspace and cyber warfare have enabled the transformation of military operations into a style that more effectively integrates the benefits of the cyber domain. With the increasing advancements in technology, and the timeless thirst for information to support the decision-maker, Network Centric Warfare emerges.

Network Centric Warfare

Network Centric Warfare means many things to many people. It is not cyber operations or Internet-centric warfare, nor is it information warfare—although it utilises elements of all these functions.[127] It is the fusion of the information available to decision-makers at all levels to reduce the organisational stovepipes, enabling the development and application of knowledge superior to that of an adversary. The network is a conduit that connects the huge range of sensors, radios, command-and-control systems, and situational-awareness systems such

126 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030 – Defence White Paper 2009*, Department of Defence, Canberra, 2009, p. 83.

127 Lieutenant General Joseph E Hurd (USAF, retired), 'Network centric warfare and air power', Keith Brent (ed.), *Network Centric Warfare and the Future of Air Power: The Proceedings of a Conference held in Canberra by the Royal Australian Air Force, 16–17 September 2004*, Air Power Development Centre, Tuggeranong, 2004, p. 23.

as blue force tracker and data links. The network—or more accurately networks—allow the transfer of information to the appropriate decision-maker. Network Centric Operations enable a more focused use of information so that decision-makers and operators can conduct more effective warfare. In fact, the United Kingdom may be more accurate in its labelling of this style of warfare as Network Enabled Capability.[128] Network Centric Warfare will require a broadening of the relationship between humans, technology, and cyberspace in military operations.[129] David Alberts and Richard Haynes argue that power occurs where the greatest means and opportunity for influence can be applied; that Network Centric Warfare has enabled a decentralised shift, or movement closer to the edge.[130] Enabling greater influence at the edge of the network web enables a decrease in stovepiping of information, increasing the power and influence of the organisation over an adversary.[131]

Network Centric Warfare is not centred on technology but on the decision-maker and the operator. An adversary who blends into the general population can nullify the best sensor-to-shooter process. This means Network Centric Warfare is not just a shift to high-end technology, but a move to technology that fits the context of the operational environment. The goal of Network Centric Warfare is superior decision-making, leading to superior influence over the adversary. Network Centric Warfare is about using the right technology at the right time to meet informational requirements. If that means using a contracted agent sitting on a hill with a satellite phone rather than a billion-dollar imagery satellite, then so be it. All other activities are peripheral to getting inside the adversaries' decision cycle—their OODA loop—so the shape and tempo of operations are shaped favourably towards a friendly advantage.[132] Thus, Network Centric Warfare is a people-centric activity supported by technology, processes, and cyber operations.[133]

---

128 Air Vice-Marshal Iain McNicoll, RAF, 'Network centric warfare – perspectives from the United Kingdom', Keith Brent (ed.), *Network Centric Warfare and the Future of Air Power: The Proceedings of a Conference held in Canberra by the Royal Australian Air Force, 16–17 September 2004*, Air Power Development Centre, Tuggeranong, 2004, p. 37.

129 Air Marshal Angus Houston, 'Keynote address: the future of air power – RAAF response to the ADF Roadmap', Keith Brent (ed.), *Network Centric Warfare and the Future of Air Power: The Proceedings of a Conference held in Canberra by the Royal Australian Air Force, 16–17 September 2004,* Air Power Development Centre, Tuggeranong, 2004, p. 19.

130 David S Alberts & Richard E Hayes, *Power to the Edge: Command…Control…in the Information Age*, Information Age Transformation Series, CCRP Publication Series, Washington, DC, 2003, pp. 166–70.

131 ibid., p. 177.

132 Houston, 'Keynote address: the future of air power – RAAF response to the ADF Roadmap', pp. 10–11.

133 ibid., p. 10.

Network Centric Warfare is not the same as cyber operations, though many of its core features will rely on cyberspace. Cyber operations enhance the collection and distribution of information in and through the cyberspace domain. Intelligence, surveillance and reconnaissance systems are producing greater levels of information, but unless that information is channelled to the decision-maker or operator in a timely manner, its value reduces rapidly.[134] Cyber operations and cyberspace are the conduits to get the information to the right people at the right time, regardless of their physical location. Offensive cyber operations can provide insight into the adversary's decision space, while defensive cyber operations will maintain information assurance and reduce the risk of disruption to the information flow. Cyber operations are essential to military operations and the development of Network Centric Warfare, but they are an enabler, an element of the larger concept, not the concept itself.

Network Centric Warfare does not change the military's strategic reasons for being, nor does it change the Clausewitzian nature of war. Violence, chance and uncertainty will continue to pervade all facets of conflict; however, Network Centric Warfare can sway chance towards those with superior decision-making and reduce, not erase, some of the fog of war.

Summary

Clausewitz and Sun Tzu are alive and residing in the depths of cyberspace. Indeed, they may have written their dictums for conventional warfare, but their strategic guidance is as timeless as Aristotelian philosophy. Society is firmly plugged into cyberspace with nearly every facet of human activities reliant upon it in some way. Clausewitz's trinity of government, military and the population captures both the interconnectivity of society and the strategic interdependence each side of the trinity has on cyberspace. Equally, Sun Tzu understood the importance of information and the effect it has on success in war. He appreciated the value of indirectness, the role of deception, and the significance of information secretly collected on an adversary's capabilities. Cyber operations facilitate all these activities. Cyber operations include all activity, friendly or adversarial, conducted to achieve desired objectives in or through cyberspace. These activities include cyber attack, cyber defence, and support to cyber-enabled capabilities such as command-and-control systems.

Cyberspace is its own and unique warfighting domain, sitting not separately from but across the physical domains of air, land, sea and space. The core element of cyberspace is information. In the military environment, information operations integrate the employment of a series of core, supporting and enabling capabilities

134 Waters, Ball & Dudgeon, *Australia and Cyber-Warfare*, p. 7.

to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.[135] The military cyber element of information operations is computer network operations, which is broken into computer network attack, computer network defence, and computer network exploitation. Military cyber operations are critical to the freedom of manoeuvre in cyberspace, but the full potential of cyber operations occur when military cyber operations are integrated with the other elements of national power, such as the Australian Defence Force, and the vivacity provided by the public sector.

The Australian Defence Force, along with many modern militaries, is exploiting the benefits inherent in cyberspace to transform its operational methodologies. Land forces have long embraced the concept of mission orders, decentralising control and execution to the furthest edges of its command chain. The length of this chain has always been limited by information systems and the ability to rapidly gain situational awareness of the tactical, operational and strategic environment. Network Centric Warfare removes stovepipes, stretches the chain of influence out further, and flattens the organisational model, thereby gaining information superiority and getting inside the adversary's decision-making cycle. Cyberspace and cyber operations are elements essential in bringing about this transformation, but they are not the only elements. The focus of Network Centric Warfare is the human decision-maker. All the technology, processes and communication infrastructure are peripheral to the people for whom the information is intended. The right information at the right time can be turned into decisive knowledge if supplied to the right person. Network Centric Warfare seeks to harmonise all the elements that provide information and build the knowledge base sufficiently to push power to the edge.

135 United States Joint Chiefs of Staff, Joint Publication 3-13: *Information Operations*, p. GL-9.

Chapter 4

Cyber Australia

Like other modern nations, Australia is wired to cyberspace. BlackBerries, iPhones, cable television, Facebook, and online banking are accepted parts of the Australian culture, and all rely on cyberspace for their continued existence. With a few cleverly placed lines of code, all these could disappear, at least for a period of time. Admittedly, most of these items are convenient to Australia's lifestyle and not critical to her national security interests. So how much does cyberspace fuel those interests Australia considers vital to the stability of its national security environment? Moreover, what would happen if that fuel was cut off or contaminated? Who has the responsibility for maintaining the free flow of information that fuels Australia's security interests and blocking contaminants from infecting the national security engines?

This chapter lays out the chain of responsibility for Australia's national cyber security that runs from the Government to the individual. An overview of Australia's national security environment provides an appreciation of how and why the various responsibilities for elements of the cyber domain developed. At the pinnacle of national strategy is the 2008 Prime Ministerial National Security Statement from which the 2009 Defence White Paper, *Cyber Security Strategy*, and other national security documents took their guidance. The buck for national security ultimately stops at the Prime Minister, but the process to support the maintenance of cyber security is multifaceted. Each nation's security interests vary with its security environment and domestic organisation. Understanding what national security means to Australia is the first step to understanding Australia's approach to cyberspace.

What is National Security to the Australian Government?

The 2009 Australian Defence White Paper contends national security 'is concerned with ensuring Australia's freedom from attack or the threat of attack, maintaining our territorial integrity and promoting our political sovereignty, preserving our hard-won freedoms, and sustaining fundamental capacity to

advance economic prosperity for all Australians'.[136] National security supports Australia's strategic interests, of which the highest priority is the defence of Australia against direct armed attack, either by states or by non-state actors with strategic capabilities such as weapons of mass destruction (WMD).[137] Professor Hugh White, Head of the Strategic and Defence Studies Centre at the Australian National University, argues that the highest priority strategic interest, and the primary role of Defence, is to 'hedge against the risk that a collapse in the international order in Asia over the next few decades might sharply increase the risk of conventional conflict'.[138] Cyber operations can neither prevent the collapse of international order nor stop a direct armed attack, but they can disrupt an adversary's capabilities and assist in providing some degree of strategic warning.

The second priority is the security, stability and cohesion of Australia's nearest neighbours. Combined cyber operations can prove mutually advantageous by enhancing elements of other nations' information systems and standardising defensive measures, thus securing greater cooperation and increased security. Countries in Australia's neighbourhood that feel secure are less likely to conduct asymmetric growth in offensive capabilities or host powers unfriendly to Australia due to a perception of a security imbalance.

If the world is in chaos, Australia will not be able to sit in its corner of the world and feign stability. Stability in the broader Asia-Pacific region, and a stable, rules-based global security order, are the next significant strategic interests.[139] Australia is proactive in the region in the promotion of stability, and its approach mirrors its current attitude to national security.

Approach to national security. Diplomatic, economic and informational support to maintain a stable global and regional environment is Australia's best solution to preserving national security; however, under the norms of international law and United Nations obligations, Australia will, if required, use force to establish and maintain its national security.

---

136 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030 – Defence White Paper 2009*, Department of Defence, Canberra, 2009, p. 20. This position on national security mirrors the definition presented by Prime Minister Kevin Rudd in his 2008 National Security Statement to Parliament.

137 ibid., p. 41.

138 Hugh White, 'Security, prosperity, and defence', William Maley (ed.), *Australia's Security and Prosperity: Ideas for 2020*, Department of International Relations, College of Asia and the Pacific, Australian National University, Canberra, 2008, p. 17, viewed 23 March 2011, <http://ips.cap.anu.edu.au/ir/pubs/keynotes/documents/Keynotes-9.pdf>.

139 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030 – Defence White Paper 2009*, pp. 42–43.

Australia will pursue means other than military force if the security situation enables such a response.[140] This approach was evident during Australia's intervention in East Timor during the 1990s. Significant effort was undertaken in the United Nations, as well as directly with Indonesia, to support East Timor's push for self-determination. The world media highlighted the East Timorese struggle for independence, and Australia strengthened its economic ties with both Indonesia and the East Timorese in a bid to reduce the tension. With mounting violence threatening to destabilise the region, Australia, with Indonesian permission and under the flag of a United Nations-sanctioned peacekeeping mission, entered East Timor to conduct military operations to stabilise the region. Force is the least preferred approach, but utilised when the national security environment evolves to a point where other options are unworkable.

National Security Environment

Global. The potential for a war between the major powers is considered remote, with trade interdependencies and other shared concerns such as transnational crime, global terrorism, and drug markets reducing the risk. However, unforeseen breakdown in international relations or a change of domestic politics can lead to tensions that could rapidly escalate into hostilities; thus the possibility of a major war, though distant, cannot be ruled out.[141]

Intra-state. Armed conflict short of conventional war will be the most common form of dispute that will influence Australian's national security interests in the period out to 2030. Combat operations, typified by counterinsurgency, stabilisation, or peacekeeping, will reflect the most common style of operations Australia's military forces will be prepared to undertake.[142]

Non-state actors. Terrorist groups, drug cartels and crime syndicates are not an existential threat to Australia's national security, but these groups can undertake localised activities that harm Australian citizens or property, undermining the population's confidence in the government. This threat amplifies if non-state actors attain WMD, or conduct nationwide cyber attacks.[143]

Asia-Pacific region. Current trends indicate the Asia-Pacific region will weather the current global financial crisis with some impacts to short-term gross domestic profits. However, in the longer term, a renewed sense of shared purpose and strategic interests may emerge, building regional stability and enhancing each

140 ibid., p. 20.

141 ibid., pp. 21–22.

142 ibid., p. 22.

143 ibid., p. 24.

country's national security.[144] Australia's national security is linked to stability in the Asia-Pacific region. The greatest risk to regional stability will be a shift in the power relationship between China, US, Japan, India and Russia that could increase tension in the regions and generate instability. Regional countries will align with different powers and, as tension increases, may resort to cyber operations as a means to influence other nations without crossing the threshold into armed conflict.

Jumping the air-sea gap. The 2009 Defence White Paper states, 'The enduring reality of our strategic outlook is that Australia will most likely remain, by virtue of our geostrategic location, a secure country over the period to 2030. We are distant from traditional theatres of conflict between the major powers, and there is an absence of any serious, enduring disputes with our neighbours that could provide a motive for an attack.'[145] Figure 4–1 depicts the geographic divide that exists between Australia and its regional neighbours, with the air-sea gap highlighted in the insert standing as a barrier to physical forces. While Papua New Guinea stands as Australia's closest neighbour, its terrain is unsuitable for mounting a significant land campaign; as Japan discovered during World War II. Unfortunately, Australia's maritime approaches present no barrier to a cyber attack. Actors who wish to use force, but do not have the physical capability to bridge the air-sea gap to Australia's north, may resort to cyber attacks as a means to dispense violence on the Australian populous.[146] The Australian Defence Force has the responsibility for securing the air-sea gap, but who has the responsibility for securing the cyber gap?

144 ibid., p. 33.

145 ibid., p. 49.

146 Violence in the context discussed in Chapter 2.

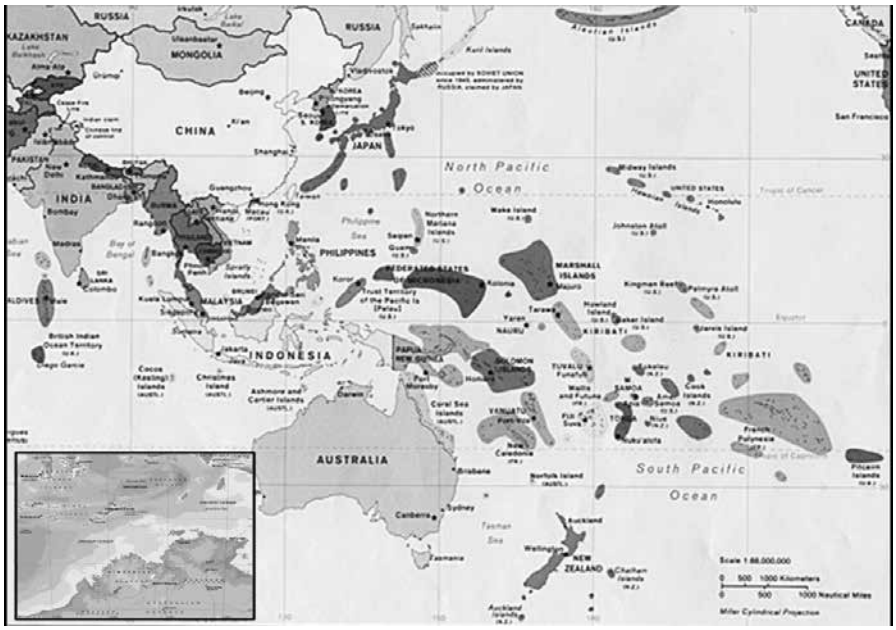

Figure 4–1: Australian geographic environment with northern air-sea gap insert[147]

Australia's National Security Statement

National Security Statement. In 2008, Prime Minister Kevin Rudd delivered Australia's first National Security Statement. This Statement provided a national security policy framework from which a Government reform agenda would sustain the security of Australia's national interests.[148] In lieu of a documented strategy, Ric Smith, the author of a report that provided the foundation for the Statement, asserted that future national security needs could be addressed

147 Source: Maps adapted from <http://easttimorlegal.blogspot.com/2011/01/timor-sea-program-amendment-gets-ok.html> and <http://mappery.com/East-Asia-and-Oceania-Political-Map>, viewed 26 March 2011.

148 Prime Minister Kevin Rudd, *The First National Security Statement to the Australian Parliament – Address by the Prime Minister Of Australia The Hon. Kevin Rudd MP, 4 December 2008*, Department of the Prime Minister and Cabinet, Canberra, 2008, p. 39, viewed 23 March 2011, <http://www.iseas.edu.sg/aseanstudiescentre/ascdf3_Rudd_NatSec_041209.pdf>.

through periodic statements by the Prime Minister, and by the articulation of the Government's strategic priorities.[149] The Statement outlined the current strategic environment around which the national security agenda is framed. Amongst concerns such as defence against physical attack, transnational crime, and border protection, the Statement postured cyber security as a high priority on the Government's agenda and list of initiatives.

Strengths and weaknesses. Through the Statement, the Government undertook a number of excellent initiatives, such as the establishment of the Cyber Security Operations Centre and the Computer Emergency Response Team, which will enhance Australia's resistance to cyber attack. Unfortunately, the 2008 National Security Statement does not provide a framework for a security strategy, but a framework for the development of a series of White Papers that suffer from lack of strategic integration. Individually the White Papers are excellent documents that clearly set out that Department's individual strategy to support national security interests. However, a lack of documented executive guidance limits the ability to articulate fully the authoritative responsibilities, integration processes, and coordination required if a National Security Community is to develop into an effective entity—one capable of undertaking a whole-of-government response to a crisis.[150] The buck may stop at the Prime Minister if a serious national security event such as a national cyber attack occurs, but subordinate echelons will share plenty of blame. Ric Smith alludes, 'While crisis management by the [Australian] Commonwealth has generally been done well "on the day", the current hazard-specific approach and the absence of consistent national arrangements for handling significant crises exposes the Government to several areas of vulnerability' and 'Emergency management across all hazards has received limited senior attention within the Commonwealth'.[151] Effective response to any national security crisis, such as an Estonia-style cyber attack, begins with robust strategic guidance. The National Security Statement provided some guidance from which the 2009 Defence White Paper developed a strategy that enables a national response to potential future crises.

---

149 Ric Smith, *Report of the Review of Homeland and Border Security: Summary and Conclusions, 4 December 2008*, Government of Australia, Canberra, 2008, p. 2, viewed 23 March 2011, <http://www.royalcommission.vic.gov.au/getdoc/0be3af5e-16eb-4ba5-93c0-b83cb3a55860/TEN.004.002.0431.pdf>. This report formed the foundation for the 2008 National Security Statement.

150 John Blackburn & Gary Waters, *Optimising Australia's Response to the Cyber Challenge*, Kokoda Papers No. 14, The Kokoda Foundation, Canberra, 2011. Blackburn and Waters refer specifically to an integrated cyber strategy, but integration throughout all national security strategy is essential.

151 Smith, *Report of the Review of Homeland and Border Security,* pp. 3 and 4.

National Security Strategic guidance. The Defence White Paper states, 'Defence is one element of our broader approach to national security, underpinning our capacity to act in the world by providing options when Government contemplates the use of force'.[152] There is no argument with this statement; however, Australia is yet to publish a National Security Strategy, which would provide the 'broader approach'. Defence is a vital component to the security of Australia, and the White Paper provides a clear approach for how Defence plans to approach future strategic challenges but, as the paper indicated, Defence is just one element. Without a hierarchical, authoritative document, other governmental organisations, as well as the private sector, have little guidance on the Government's plan for the integration of all elements into the broader security environment. The US learnt in the aftermath of the 9/11 tragedy that a national strategic approach to security is essential, and the lack of strategic direction, in their case across their intelligence organisations, contributed to gaps in their national security. Security requires a whole-of-government—indeed a whole-of-society—approach. How is Defence to integrate with elements of the Departments of Foreign Affairs and Trade, Immigration, Treasury, and Attorney-General, or the private and public sector to provide national security? The reciprocal can be asked of each of these organisations as well. In the event of a national security incident who has responsibility for what? What if this incident is cyber-based? What is the ADF's role? These questions will be addressed in this chapter.

In the National Security Statement, the Prime Minister acknowledged Australia's growing vulnerability to cyber attack from foreign states, as well as commercial, criminal and self-interest actors, due to the reliance on information to 'lubricate our economy and system of government'.[153] The challenge the Government faces is determining the magnitude of consequences a major cyber attack would have on Australia's economic, social and military environment; herein lies some of the problem. It is very difficult to gauge the degree of disruption, damage, corruption or destruction a cyber attack has on a particular information system. Unlike a kinetic attack where destruction is almost immediately measurable, effects from cyber attacks may be masked or illusory. During the 2010 Stuxnet cyber attack on the Iranian nuclear facility, the operators were reportedly not even aware an attack was occurring due to the masking effects of the virus.[154] Even with situational awareness of a cyber attack, second and third-order consequences may not be appreciated. Using the Iranian attack as a hypothetical example, the attacker's goal may have been to demonstrate the ability of an outside party to take over certain

---

152 Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030 – Australian Defence White Paper 2009*, p. 20.

153 Rudd, *The First National Security Statement to the Australian Parliament*, pp. 23–24.

154 'The Stuxnet worm; Yet to turn', *The Economist*, 16 December 2010, viewed 6 February 2011, <http://www.economist.com/node/17730556>.

control functions from the Iranians. The complexity of cyberspace could have resulted in unforeseen software corruption, triggering an unintended crash of the nuclear fuel-rod cooling system, resulting in a nuclear meltdown and widespread radiological contamination. Understanding the complexities of cyberspace, the vulnerabilities it brings with its advantages, and the impact of consequences orders of magnitude below the observed effect are special responsibilities the Commonwealth has in the development of the national security policy and strategy.[155] It is therefore critical for the clarification of roles and responsibilities during all cyber operations to avoid confusion and duplication of effort.

New level of leadership, direction and coordination. Given Australia's size and current available expertise, the Government elected to reinvigorate the leadership, direction and coordination among the current agencies rather than develop new organisations. Improved integration and information sharing, alongside better strategic planning and coordination will deliver a synergistic approach to national security.[156] Ric Smith emphasised the need to strengthen interagency ties when he advocated, 'While Australian Government agencies are committed to whole-of-government performance and generally understand their roles in the broad national security community, there is a need for an overarching policy framework and for strategic direction. Such a framework would better equip the Government to plan and evaluate the activities of agencies and to ensure targeted resource allocation that reflects current priorities.'[157] The National Security Statement presented the opportunity to describe publicly a framework upon which all agencies develop a whole-of-government approach to security; however, as argued previously the Statement did not provide a strategy to build such a framework. This does not mean a strategy or framework does not exist. Guidance from the National Security Committee of Cabinet or the Secretaries Committee on National Security could provide strategy guidance in confidential documents. The Secretaries Committee on National Security, known as SCNS, remains the lead Australian interdepartmental committee on national security policy and operational matters. SCNS coordinates the implementation of the Government's security policy directives and provides advice to the National Security Committee of Cabinet on departmental national security issues.[158]

Australian Attorney-General – the cyber prince. Cyber Australia does not have a cyber czar responsible for all national cyber-related issues, but the Australian Attorney-General has the portfolio to coordinate security and emergency management activity, including cyber activity. A cyber czar is not necessary

155 Smith, *Report of the Review of Homeland and Border Security*, p. 4.

156 Rudd, *The First National Security Statement to the Australian Parliament*, p. 33.

157 Smith, *Report of the Review of Homeland and Border Security*, p. 2.

158 Rudd, *The First National Security Statement to the Australian Parliament,* p. 37.

in the Australian context as the Government aims to normalise cyber security as just another element of security, rather than to hold it up as a beacon for the moths to attack.[159] The *Cyber Security Strategy* states that the 'Attorney-General's Department is the lead agency for cyber security policy across the Australian Government and chairs the Cyber Security Policy and Coordination (CSPC) Committee, which is the interdepartmental committee that coordinates the development of cyber security policy for the Australian Government'.[160] This places the Attorney-General largely responsible for measures relating to the security, availability and integrity of all government information that is processed, stored, and communicated by electronic or similar means.[161] This responsibility does not mean the Attorney-General's Department actually conducts cyber operations, but it does provide interdepartmental guidance. Much of this guidance is formalised in the 2009 *Cyber Security Strategy*, which details, 'how the Australian Government is harnessing the full range of resources to help protect government, business and individual Australians. It describes how new capabilities have been created to help Australians, and the businesses they transact with, be better protected.' [162] In line with the National Security Statement, the *Cyber Security Strategy* breaks down the responsibilities of the Government and private and public sectors.

Cyber Security Strategy

Responsibility for cyber security is broken into four areas: Government, critical national infrastructure, private sector, and the public sector. The *Cyber Security Strategy* asserts that users in the cyber environment should take appropriate actions to secure their own systems and exercise attention to the transmission and storage of information.[163] Cyber security entails shared responsibilities, and Australia's cyber strategy is braced by a partnership approach to cyber security across all Australian governments, the private sector and the broader Australian community.[164]

Government. Responsibility for the dot-gov domain, including Defence, lies with government. The government information systems, and the information residing

159 Blackburn & Waters, *Optimising Australia's Response to the Cyber Challenge*, p. 20.

160 Attorney General, *Cyber Security Strategy*, Attorney General's Department, Canberra, 2009, p. 8.

161 Attorney-General's Department, 'E-Security', Attorney-General's Departmental website, viewed 27 March 2011, <http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_E-Security>.

162 Attorney-General, *Cyber Security Strategy*, p. i.

163 ibid., p. 8.

164 ibid.

within them, are strategic national assets.[165] Because the government owns these systems, it has mandated minimum security standards that apply across all departmental information systems.[166] However, Australian government systems represent only a small percentage of the information systems on which economic and national security depend.[167] Most prodigious are those information systems belonging to the public and private sectors, while the most vulnerable are those supporting the nation's critical infrastructure.

Critical infrastructure. Critical infrastructure delivers essential services such as power, water, health, communications systems and banking.[168] It is Australian policy that the Government, owners and operators share the responsibility for the continuity of critical infrastructure.[169] Not all infrastructures are hardware or cyber-based, with many elements consisting of networks or supply chains. Bringing electricity from the power plant to the fax machine involves linking many physical and cyber-based elements involving a complex network of producers, control systems and distribution infrastructure.[170] The Australia Government has adopted a dual approach to facilitating the security of critical infrastructure.

The first step is the implementation of the *Critical Infrastructure Resilience Strategy* in 2010. This strategy seeks to reduce the risk of disruption of services delivered by the critical infrastructure through assisting the owners and operators to better manage 'both foreseeable and unforeseen or unexpected risks to their critical infrastructure assets, supply chains and networks'.[171] A key initiative of this strategy is the Trusted Information Sharing Network, a forum where the owners and operators of critical infrastructure work together with government, sharing information on the security issues that affect them. The focus of this approach is to empower the owners and operators of critical infrastructure to strengthen and improve their security measures and to help inform their risk management.[172]

At the heart of critical cyber infrastructure are the supervisory control and data acquisition (SCADA) systems, devices and networks used to electronically control mechanical processes such as the generation and transmission of electricity. Because of the complexity of modern critical infrastructure, SCADA systems are

---

165 ibid., p. 21.

166 ibid.

167 ibid., p. 14.

168 Attorney-General, *Critical Infrastructure Resilience Strategy*, Attorney General's Department, Canberra, 2010, p. 3.

169 ibid.

170 ibid., p. 8.

171 ibid., p. 4.

172 Attorney-General, *Cyber Security Strategy*, p. 20.

the cyber Achilles heel towards which a cyber attack would be focused. The *Cyber Security Strategy* and the Trusted Information Sharing Network seek to increase the resilience of Australia's critical infrastructure to disruption or damage from any risk, including attacks from the cyber domain.[173]

Private sector. The business community bears the responsibility for the security of their information systems.[174] Business owners and operators—the dot-com/dot-org/dot-au domains—must manage their own risks; however, the Government accepts a responsibility to assist the private sector to understand and mitigate the threats they face.[175] In particular, the *Cyber Security Strategy* commits the Government to actively participating in and facilitating trusted and timely information sharing within and between government and business.[176] The Government's goal is for Australian businesses to operate secure and resilient information systems to protect the integrity of their own operations and the identity and privacy of their customers.[177] In the event of a major cyber attack on the private sector, the Government has laid out where the responsibility lies for cyber security; however, it is arguable whether the private sector knows where to turn if the power shuts off, its mobile phones cut out, Facebook freezes, or retirement funds disappear.

Public sector. Like the private sector, it is the policy of the Australian Government that individuals in the public sector bear the responsibility to 'ensure their personal and financial information and their identity and privacy are protected. It is essential that they maintain an awareness and understanding of the cyber environment and its risks'.[178]

CERT. In partnership with the private sector, the Government is committed to educating Australians on cyber security risks and empowering them with the knowledge to reduce the risk from cyber threats.[179] A key initiative mandated in the National Security Statement and enacted through the *Cyber Security Strategy*, is the Computer Emergency Response Team (CERT). CERT, which falls under the responsibility of the Attorney-General, will educate the public and private sectors on cyber threats and provide information on how to better protect themselves.[180] It will also be another avenue for owners and operators of critical infrastructure to

---

173 ibid., p. 13.

174 ibid., p. 11.

175 Smith, *Report of the Review of Homeland and Border Security*, p. 6.

176 Attorney-General, *Cyber Security Strategy*, p. 15.

177 ibid., p. vi.

178 ibid., p. 17.

179 ibid., p. 10.

180 ibid., p. 9.

seek advice on reducing threats to their services. The Government has promoted CERT as a one-stop shop for advice and education, but with no advertised authority to take direct action against a cyber attack on the public or private sector. If this is the case, then the population should be asking what response they could expect in the event of a cyber-based (computer) emergency.

Regulation. The Australian Government views its role in the public and private sector as promoter of a robust culture of cyber security, educating the population on how to protect themselves rather than directing the public and private sectors on the measures they must take via regulation. This is akin to teaching a group to farm so they can sustain themselves.

So why not more regulation? The Australian Government is the industry regulator in other sectors, such as aviation and maritime, so why not legislate cyber security standards for the public and private sector, as they have for the governmental departments?

Australia's non-regulatory approach is formulated around the premise that the owners and operators of information systems understand the risks to their operations and have an inherent self-interest to mitigate the risks. In its *Critical Infrastructure Resilience Strategy*, the Australian Government asserted that regulations are 'not suitable for critical infrastructure as the identification of minimum-security benchmarks or regulations across industry can be difficult, even within specific sectors.'[181]

However, it is of concern that in a sector where the consequence of a cyber attack could be widespread and debilitating to the national security environment, the onus for mitigating the risk falls on those having to balance the profit margins. Alastair MacGibbon argues that self-regulation has a shaded history with numerous examples of failure in the telecommunications sector.[182] Many of the initiatives put in place by industry have been reactionary to a crisis rather than precautionary. In an economically challenged environment, this is difficult to justify to the shareholders spending large amounts of capital on problems that may never arise.

Given the cost of a successful cyber attack on a critical infrastructure SCADA system, should not a trust-but-verify strategy be considered? In a liberal democracy, freedom has its risks.

---

181 Attorney-General, *Critical Infrastructure Resilience Strategy*, p. 14.

182 Alastair MacGibbon, 'Cyber security: threats and responses in the information age', Australian Strategic Policy Institute, *Special Report Issue 26*, December 2009, viewed 24 March 2011, <http://www.aspi.org.au/publications/publication_details.aspx?ContentID=233>.

Government Cyber Operations

The *Cyber Security Strategy* clearly articulated that the Government has the responsibility for 'the security and resilience of its own ICT [information communication technology], including protecting the information it holds about Australian people and organisations.'[183] The Government looks to achieve this objective through the education of governmental employees on cyber threats and their responsibilities in security processes, extensive security protocols, cyber security software, and cyber hardware with built-in security components. Over the top of these actions, a set of cyber security regulations provide common cyber security standards for all departments in an attempt to minimise potential cyber backdoors. These institutional measures, incorporated over the past decade, enable a collective departmental approach to cyber security.

To build on these protective capabilities, the Government has designated the Department of Defence to be the operational lead on governmental cyber security operations. In the 2009 Defence White Paper, the establishment of a Cyber Security Operations Centre (CSOC) serves as a measure to maximise the Australian Government's ability to 'prevent, detect and rapidly respond to fast evolving sophisticated cyber exploitation attempts and attacks.'[184] The Centre will provide government with a broad understanding of cyber threats against national interests; and, with representatives from Defence and the broader national security community, will coordinate whole-of-government responses to cyber events of national importance across government and critical infrastructure.[185] The CSOC will be the tip of Australia's cyber sword in its fight to maintain freedom of access across the cyberspace domain. As depicted in Figure 4–2, the Centre, established in the Defence Signals Directorate (DSD), provides Defence with a cyber warfare capability through the conduct of computer network operations, and a resource designed to serve all government agencies. It is important to note that the term '*in*' has been used explicitly in all the government documents to indicate that while the Centre is located inside a Defence establishment, it is not just for the sole use of Defence, but also acts as a whole-of-government resource. The Defence Signals Directorate is an excellent choice of location as it has a long history in information operations, and is a venue well adapted to the classified nature of this style of operations.

183 Attorney-General, *Cyber Security Strategy*, p. 14.

184 ibid., p. 28.

185 ibid., p. 9.

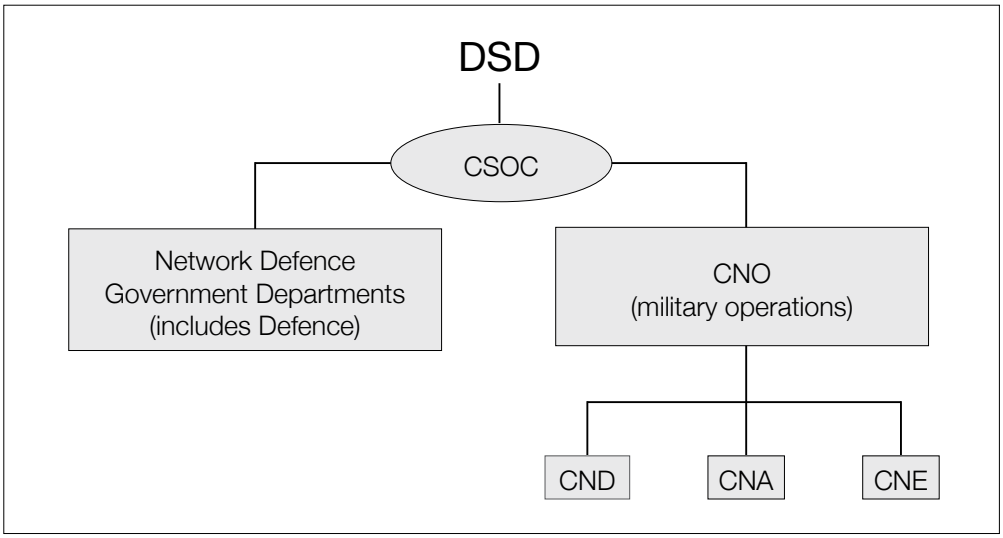

Figure 4–2: DSD/CSOC strategic and operational cyber security responsibilities[186]

Defence Signals Directorate. The Defence Signals Directorate (DSD) is the national authority on the security of information systems across government. DSD has a mandate to ensure that sensitive government information systems are not susceptible to unauthorised access, compromise or disruption.[187] DSD's mission statement, 'Reveal their secrets – Protect our own', reflects the essence of cyber operations: the Clausewitzian duality of offence and defence, required for success in any war.[188] It is a motto that would fit easily into Sun Tzu's estimates on the waging of war.

Summary

Cyberspace is a primary enabler for Australia's economic and social wellbeing. It permeates nearly every sinew of the Australian Government and the private and public sectors, and underpins the delivery of essential services from critical infrastructure. The efficiencies gained from the exploitation of cyberspace have enabled Australia to continue its journey through the 21st century as a leading nation in technical, trade, financial and military affairs in the Asia-Pacific region.

186 Source: Author's original work.

187 Attorney-General, *Cyber Security Strategy*, p. 29.

188 Defence Signals Directorate, 'Cyber Security Operations Centre (Australia)', Department of Defence, Canberra, 2010, p. 15.

With every upside there is invariably a downside, and the reliance on cyberspace has made Australia vulnerable to actors who seek to undermine its wealth and security.

The Australian Government considers the greatest existential threat from a direct armed attack against the mainland, though it acknowledges the risk of this occurring is low. The air-sea gap to Australia's north provides a formidable barrier to any physical attack, but it offers no more resistance to a cyber attack than a sandcastle to an incoming tide. It is Australian policy to resolve threats to national security, which include attacks or regional instability, by means other than force. However, if required, the Government has demonstrated its will to apply force, as it did in support of East Timor's 1999 bid for self-determination. The Australian Defence Force is responsible to the Government for the protection of Australia from hostile forces, but as the influence of cyberspace pervades all sectors of life, the responsibility for security is segregated. The Government maintains direct responsibility for the protection of all information under its purview, while all organisations and individuals in the public and private sector, as well as operators and owners of critical infrastructure, bear the responsibility for the security of their cyber-based information systems. Citizens bear the responsibility for protecting themselves from a foreign cyber attack. The Government has taken on the responsibility to provide opportunities for organisations and individuals to be educated on the threat and provide advice on possible actions to mitigate the risk or respond to an attack.

The Prime Minister's 2008 National Security Statement and the Attorney-General's *Cyber Security Strategy* map out the future direction for the security of cyberspace. The *Cyber Security Strategy*, in conjunction with the 2009 Defence White Paper, outlines some key initiatives to advance Australia's readiness to combat threats against government information systems. Alongside an education process, a network of integrated information security systems, and a mandated set of security regulations, a new Cyber Security Operations Centre was established with the prime responsibility for detecting, preventing and responding to any exploitation attempt or attack on a government information system. The Centre resides in the Defence Signals Directorate, but has representation from all facets of the national security community to facilitate a whole-of-government response to any cyber crisis. If the RAAF wants to play a significant part in forging future cyber capabilities, it needs to grow its cyber representation within the Defence Signals Directorate.

The Cyber Security Operations Centre will play a critical role in the conduct of any cyber operations conducted by Defence. The extent of any cyber attack capabilities resident in Defence are classified, though both the *Cyber Security Strategy* and Defence White Paper indicate that Australia is undertaking enhancements in cyber warfare. Cyber attack is unlikely to be employed as the sole capability in any military operation, but during the shaping phase of an

operation, Defence may employ cyber attack to minimise the logistic footprint in an area of operations, while still undertaking influence operations.

Chapter 5

The Australian Military Through the Cyber Looking Glass

Cyber security means more than putting up firewalls. It entails a range of actions to ensure the continuance of a state's sovereignty and the freedom to pursue national interests. The Australian Defence Force has the responsibility of providing the security to protect the nation from attacks that threaten the national interests or the continuance of sovereignty. Defensive measures form a large part of the provision of this security. Clausewitz states defence is the strongest form of fighting, but if words give way to actions, offence is the only method that ensures the achievement of national objectives.[189] This argument holds true in the cyber domain where the ADF's focus is on defence, but in the face of a persistent adversary or mass of individual attackers, defence must be balanced with elements of attack if security is to be maintained. The previous chapter asserted that the Australian Government considers the security of cyberspace a shared responsibility with all elements of the Australian population. The public and private sectors, not the ADF, have the responsibility for establishing adequate defensive measures to protect the information systems they own or operate. To these sectors, the Government considers that its responsibility is to provide advice on potential threats and options to combat these threats; it meets these responsibilities through the provision of the Computer Emergency Response Team and cyber information websites. In the area of critical infrastructure, where delivery of essential services is vital to the maintenance of Australian societal norms, the Government goes a step further in the level of advice by providing close-hold information on threats and protective measures through the Trusted Information Sharing Network. Nonetheless, the primary responsibility for the protection of information lies with the owner and operator of the information

189 Carl von Clausewitz, Michael Eliot Howard & Peter Paret, *On War*, rev. ed., Princeton University Press, Princeton, NJ, 1984, p. 84.

system. The same stance holds true with information systems owned and operated by the Department of Defence.

Policymaking for the protection of Government information falls under the realm of the Attorney-General, but responsibility for conducting operations that meet the policy's aims falls to the Department of Defence. Government information covers the information systems across all federal governmental departments, including Defence. Each department employs information technology officers to oversee compliance with local regulations and federal mandates, but the gatekeeper for the flow of information into and out of the global information grid (GiG) is the Cyber Security Operations Centre, located in the Defence Signals Directorate (DSD) in Canberra. The Department of Defence responsibilities in cyber security can be broken into two elements: cyber operations in support of government information systems, and computer network operations in support of military operations. While there is an increasing appreciation of the importance of cyber to ADF operations, the development of cyber capabilities within the ADF lags the growing reliance that combat capabilities have on the cyber domain. Much of the ADF and Service cyber activity occurs within the classified realm, so the full extent of the ADF's activities cannot be revealed. The ADF is working hard to play catch-up to protect its capabilities and exploit cyberspace to gain operational advantages. Cyber developments in the Army and Navy closely mirror those of the RAAF and are not addressed within the scope of this paper. However, because cyber permeates across all the warfighting domains, the RAAF must coordinate and integrate its cyber development activities with all Services, as well as with the broader joint and whole-of-government cyber organisations. This chapter looks broadly at the development of cyber operations in the ADF but, as a prelude to developing the future direction for Air Force cyber operations, focuses on the implications of cyber for the RAAF.[190]

Cyber and the ADF

Cyber operations permeate all the warfighting domains, and because modern warfare levers much of its capacity to engage in operations from cyber, the conduct of military cyber operations should be inherently a joint function. The ADF understands the importance of cyber to its future effectiveness as a fighting force. Through Network Centric Warfare (NCW), the ADF is undertaking a long-term transformation of its entire warfighting system to enable it to fight as a whole rather as individual parts. The ADF's cyber operations are an important enabling function of NCW as they enable the use of networks to provide connectivity

190 Most of the ADF's cyber operations are classified, or in such a developmental stage that is not releasable. Information on ADF cyber operations is predominately drawn from unclassified interviews.

between distributed commands, units and individuals, and the fusion of information that resides within the networks. NCW will align weapons platforms and individuals to share information appropriate to the differing strategic, operational and tactical missions. However, as established previously, cyber is an enabler for NCW; cyber operations are not NCW. For NCW to develop, the ADF must undertake parallel development of its cyber operations capability. So if the ADF is to exploit cyberspace to maximise its combat effectiveness, which organisation holds the responsibility for making this happen, and what role do the Services play in this development?

At the departmental level, DSD has the responsibility for conduct of all strategic and much of the operational-level cyber operations. Under the *Intelligence Services Act 2001*, one of DSD's functions is to 'provide assistance to Commonwealth and State authorities in relation to: (i) cryptography, and communication and computer technologies'.[191] Thereby, DSD holds the majority of resources and personnel available to the Department of Defence for the conduct of computer network operations (CNO) in support of military operations. At the joint level the responsibility for conducting CNO planning and coordination falls under the J-5 Effects cell (J-5E). However, like the majority of the ADF, cyber operations planning at the Joint Operations Command is still in the development phase, and the J-5E cell is drafting a concept of operations that will eventually be the guidance principles for the conduct of joint CNO planning and execution.[192] The Australian Army and Navy have the responsibility to develop their own cyber operations personnel, but, like the RAAF, will take a number of years to develop cyber operators capable of supporting organic CNO tasking.

The joint fight

Who conducts CNO activities for Joint Task Force (JTF) and deployed components?
The J-5E will have the responsibility for the planning of all cyber operations within the theatre. The JTF and component teams lead the planning, tasking and component coordination of cyber operations, but in most cases, DSD and the Cyber Security Operations Centre in Canberra will conduct the operations. To enable reachback to occur, the JTF must be designated the supported unit and the Canberra-based centres as supporting units. Reachback is required because the personnel, infrastructure and access reside predominately in the Australia-based units. This reachback concept mirrors the arrangements that occur regularly

191 Attorney-General, *Intelligence Services Act 2001*, Office of Legislative Drafting and Publishing, Attorney-General's Department, Canberra, 2001, p. 9.

192 Flight Sergeant Karen Jenkins, telephone interview with Flight Sergeant Jenkins—CNO Supervisor J-5 Effects Cell, Joint Operations Command—conducted by Squadron Leader Craig Stallard, 3 April 2011, Montgomery, AL, 2011.

between US JTFs and US Strategic Command in the support of strategic ISR and space-based capabilities. Some elements of computer network defence (CND) can and should be deployed forward to establish familiarity with local conditions and to be responsive to the local commander. Some computer network attack (CNA) operators may be deployed forward for positive attribution purposes.[193] In an overt conflict, it may be beneficial for adversaries to be aware of who is attacking them and that the attack originated from a regional centre. A cyber attack originating within a coalition partner's state can increase the legitimacy of a coalition; thus, a forward-deployed CNA team can have both operational and strategic value. The balance of forward-deployed cyber capabilities and those available through reachback will be a source of debate, just as will be the debate over the degree of responsibilities between joint and Service cyber operations.

Joint versus Service. Joint command and control of the ADF's cyber operations is the only way to ensure the adequate defence of military information systems and an integrated approach to cyber attack and exploitation. Additionally, the size of the ADF does not lend itself to diffusing its cyber resources across too wide a span of control without diluting the available expertise in any individual unit below what is considered operationally effective. However, the Army, Navy and Air Force have a legitimate reason to establish some cyber elements within their organisations. For starters, the ADF does not have a separate cyber force that can produce joint cyber warriors and, with the constrained size of the ADF, it is not considered feasible for a separate cyber service to be established. Thus, the ADF has two choices; designate one Service to raise, train and sustain cyber operators for employment in the joint cyber community, or task the Services with the responsibility to grow cyber operators within their own organisations. The first option may seem efficient, but is not likely to proceed due to a combination of Service advocacy and a lack of experience within the single Services to support each component's targeting requirements. This leaves the second option, which is closer to the modern concept of joint organisations. Each Service grows its own cyber specialists, nurturing them in their individual Service-minded culture, so they can support individual Service and greater joint needs.

193 Wing Commander Ralp Brown, interview with Wing Commander Brown—RAF Communications Engineer, UK Ministry of Defence Desk Officer for CNO Policy R&D and Operational Planning 2007–08—conducted by Squadron Leader Craig Stallard, 29 March 2011, Montgomery, AL, 2011.

UK, Canada, Australia and US military cyber development

Australia, Canada and the United Kingdom (UK) share much common ground in the development of cyber operations. The three nations' Cyber Security Strategy concepts closely mirror each other organisationally and in process, with the opening of CSOC and CERT or equivalent centres in each country.[194] Oversight and organisational arrangements differ with different national political environments, size of military, and historical force structure, but share best practice processes. At the military level, each country is still in the early stages of cyber-operations development. Certain elements of cyber operations are available to support military actions, details of which are classified. However, there is a long process of concept-of-operations development, organisation restructuring, and growth of cyber operators at the Service and joint levels still to be conducted by each nation if the potential of cyberspace is be fully exploited.

US Cyber Command. The US is far more advanced in the exploitation of cyberspace than any of its closest allies. US Cyber Command (USCYBERCOM) stood up in 2009 and reached initial operational capability in 2010. Per its mission statement, 'USCYBERCOM plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries'.[195] Each Service has a cyber command subordinate to USCYBERCOM: Army Forces Cyber Command (ARFORCYBER), 24th Air Force (AFCYBER), Fleet Cyber Command (FLTCYBERCOM), and Marine Forces Cyber Command (MARFORCYBER). While there may be some tactical lessons that could be drawn from the development of US cyber operation, the scale of USCYBERCOM and its subordinate elements limits drawing any useful comparison that would enable the development of an effective organisation for the RAAF or ADF. Australia will continue to leverage the developments in US capabilities to grow ADF's cyber operations, and in the ADF's long tradition of growing military bonds across all the warfighting domains, Australia will do its share in the conduct of coalition cyber operations.

---

194 UK Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, The Stationery Office, London, 2009; and Minister of Public Safety, *Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada*, Ministry of Public Safety, Ottawa, 2010.

195 US Cyber Command, 'U.S. Cyber Command Fact Sheet', 2010, viewed 3 April 2011, <http://www.stratcom.mil/factsheets/Cyber_Command/>.

Cyber Operations and the RAAF

RAAF cyber objectives. Each Service has unique cyber requirements that reflect its style of operations and targeting within its primary warfighting domain. While no specific cyber objectives have been yet published, to establish and maintain its capabilities in the air domain, the RAAF needs the following four cyber-related objectives met. First, joint or Service conduct of defensive cyber operations to ensure the protection of RAAF capabilities from disruption, corruption or destruction due to cyber attacks. Second, the performance of cyber attacks in direct support of air component missions. Third, a continuance of cyber support activities, such as mission planning, intelligence and weaponeering, that are essential to the delivery of modern air power. Finally, the conduct of cyber exploitation that provides the air component commander with information that enables relative superiority in the decision-making process.

Can the RAAF gain cyber superiority? A better question may be whether anybody can gain cyber superiority. The USAF states that superiority 'prevents effective interference, which does not mean that no interference exists, but that any attempted interference can be countered or should be so negligible as to have little or no effect on operations'.[196] Superiority in cyberspace is therefore a relative term and should not be considered as an absolute; as cyberspace, more so than the other warfighting domains, is not conducive to absolute control by one party. The USAF states in its *Air Force Cyber Command Strategic Vision* that it aspires to control cyberspace, but only a sufficient level of control as to obtain local or time-limited cyber advantage for the conduct of a mission.[197] Even to gain relative superiority will take a concerted joint effort by ADF cyber operations. By itself, the RAAF should not expect to gain cyber superiority; however, in a mature joint cyber organisation the air component should expect to gain decision-making advantages through the disruption, corruption or exploitation of some elements of an adversary's information systems through support from the Joint Task Force cyber cell.

Airmindedness

Any cyber operator can employ similar types of cyber weapons, regardless of Service. The determining factor is how that weapon is employed, the type of information system, and how that weapon needs to be optimised to support a desired effect in the air domain. Here lies the difference between cyber warriors and kinetic troops. The kinetic soldier, sailor and airman use platforms and

196 United States Air Force, Air Force Doctrine Document 3-12: *Cyberspace Operations*, Department of the Air Force, Washington, DC, 2010, p. 2.

197 United States Air Force Cyber Command, *Air Force Cyber Command Strategic Vision*, Air Force Cyber Command, Barksdale AFB, LA, 2008, p. 4.

weapons optimised for the domain. Cyber warriors across all Services can use the same type of cyber weapon, but for different purposes, against different targets, and supporting different objectives. This is analogous to cyber warriors all being capable of using a cyber JDAM (joint direct attack munition), but using it in different ways for different means; a one-style kinetic weapon for all Services would not work due to the differing environments. It is not the weapon that differentiates a cyber operator among Services, but the operator's approach to targeting, support and execution of the weapon.

Objectives. Understanding the objectives and the target environment is critical to gaining the access required to undertake CNA/CNE. The complexity is in the understanding of the environment within which the information system will be accessed, and then appreciating the effect sought. At code level, a target may appear the same as any other information system; this would be analogous to looking at a circuit board with a magnifying glass—all circuit boards will look similar. Only when the view is broadened, and all the electronics are viewed, can a device be fully understood. This is where the Service-level influence comes into play. CNO experts have similar skill sets, but it is the Service-oriented experience that allows different perspectives on how to approach a problem. If an integrated air defence system is selected for a cyber attack, the air-minded cyber expert has the experience to appreciate which components to attack to achieve the desired effects.[198] An Army cyber unit may have the skill sets to conduct a cyber attack but not the individual or collective experience to conduct precision cyber attack on the integrated air defence system (IADS) to gain the required effects. The same argument holds true for an Air Force cyber team not having the experience or corporate knowledge to cyber-attack a maritime target.

There is a difference between understanding the technology and the vulnerabilities peculiar to the air domain. Cyber technicians in the ADF can be trained with the basic skills to understand the properties of the cyberspace networks common to all Services, and at face level, a cyber technician from any Service could provide the baseline defensive needs of a network. The challenge emerges as each Service seeks to adapt its networks to meet the needs peculiar to its operating environment. An Air Force cyber technician has a deeper appreciation of the cyber requirements of his/her Service and therefore can adapt basic skill sets to meet the Air Force requirements. This does not mean that all Air Force cyber technicians need to work under the umbrella of a RAAF unit; indeed having RAAF cyber staff embedded in a joint cyber unit creates excellent synergetic opportunities. However, to gain the core skill that endows them with an air-

198 Squadron Leader Duncan Scott, telephone interview with Squadron Leader Duncan Scott—Executive Officer No 462 Squadron, RAAF Information Operations Squadron—by Squadron Leader Craig Stallard, conducted 3 April 2011, Montgomery, AL, 2011.

minded perspective, the Air Force needs a cyber squadron in which to raise, train and sustain these personnel.

Differing perspectives. In the kinetic world, a desired effect may be generated by force application from different warfighting domains. For example, the Joint Force Commander (JFC) wants to stop the transmission of a cyber attack emanating from an adversary's command-and-control headquarters. The land component may advocate a direct attack on the headquarters and physically occupying the premises. Special Forces may offer a combat team to infiltrate the headquarters with the intent to either disrupt or destroy the transmitters, or conversely, convince the local cyber technicians to terminate their activities. Maritime forces may suggest a cruise missile attack to destroy the transmitter. Air could conduct aerial jamming or anti-radiation missile attacks, or destroy the headquarters with bombs. Each of these approaches can result in the same effect, but each uses a distinctive methodology, different avenues of attack, and differing second and third-degree consequences. Similarly, cyber operators from the various Services may approach the problem from their Service perspectives, conducting cyber attacks at different access approaches or even other areas of the information system. Equally, the kinetic Service attacks may seek role-specific cyber support to accomplish their mission.

Target development

Targeting. Because an adversary's software or hardware is upgradable at any time, causing loss of access to an information system or vulnerability to be resolved, cyber targeting must be very dynamic. In cyber attack, access is critical to success. Understanding the target type and the required effects can determine the avenue for access and options available to the attacker in the event one access option closes. Experience in one domain translates to effectiveness in the cyber domain. An air-minded cyber warrior brings options to the targeting and planning process that an army or maritime-focused cyber troop may not.

Cyber collateral-damage assessment. Because cyber attack is still relatively new, the rules for collateral-damage assessment for cyber operations are still maturing. In the kinetic world, the key unit of measure for collateral damage is death or injury to the civilian population. Given the long history the Air Force has with kinetic operations, and with improvements in technology and weapon-effects measurements, the physical consequences of bombs or missiles are well known. Normally the most challenging portion of kinetic collateral damage calculations is establishing the number of civil population in the vicinity of the target. The level of acceptable collateral damage will determine whether the mission will proceed. In cyber attacks, there is a very low risk of direct loss of life; however, not only are immediate consequences of the attack considered in the collateral damage calculations, but also the second and third-level effects. An example

would be a RAAF air strike on a telephone exchange. The measured collateral damage calculation would be the possible number of civilians killed or injured by the bomb. A cyber attack on the same exchange would consider not only the immediate effects of losing telephone services, but which services would be disrupted and the follow-on consequences (e.g. 911 calls may be disrupted, affecting emergency response). The RAAF needs to consider kinetic and cyber collateral damage from the same perspective, just with different methodology to achieve the same effects.

Cyber weaponeers. RAAF cyber weaponeers will have an understanding of not only the desired effects on the targeted information system, but also of potential second and third-order effects on associated systems. Given the character of cyber and its ability to pervade other domains, it is important for the air component cyber operators to have the organisational arrangements to synchronise their actions with the other components to build on the situational awareness of the cyber battlespace. Cyber actions by one component can have 'flow-on' effects to those of other components; just as kinetic air operations can affect a kinetic or non-kinetic land operation. An example of this in kinetic operations is the targeting of a bridge used as a main route for the adversary's logistic support. The Air Force destroys the bridge, disrupting the supply. A parallel land operation sought to gain intelligence from local villagers, but the destruction of the bridge cut off access to their farms; not only did the intelligence dry up, but animosity towards friendly troops grew. Cyber operations would not be immune to this type of operational miscommunication. A cyber attack on a communications hub may cut off transmission between command and control (C2) sites, but that same communications hub could have been used by the land cyber force as the means of psychological operations to inform the locals of the corruption endemic in the government and as incitement to rise up against the regime. Air-minded cyber operators might possibly understand the range of potential effects from their operations much better than cyber operators of the other Services. The RAAF must grow its cyber force so the appropriate level of airmindedness can be provided to cyber target development, planning and operational assessment in support of the air component commander.[199] All the cyber elements of the Joint Air Tasking Cycle must be supported by air-minded cyber operators. Bringing in someone from a joint pool of cyber operators to support the air component commander's objectives would equate to having an Army Tactical Missile System (ATACMS) officer conducting the weaponeering for an air strike just because he knows how to plan a precision land strike.

Collection planning. As with target development, Air Force cyber operators provide the air component collection requirements, based on the Joint Force Air

199 ibid.

Component Commander's (JFACC's) operational objectives, the air centre of gravity, and the decisive points outlined in the Joint Operation Planning Process for Air (JOPPA).[200] While the operational objectives will directly support the JFC's objectives, access analysis, target development, and operational-effect assessment require an airmindedness approach provided by the Service-component RTS (raise, train and sustain) process.

Cyber weapon payloads can be developed through the joint organisation, and likely will occur through reachback to the Australian, or coalition, organisation with the designated authority and expertise. However, payload requirements will require direction from subject matter experts with the understanding of the operational objectives, integration requirements, collateral-damage rules of engagement, and desired mission effects. These come from the operational planning team (OPT) within the requesting headquarters and therefore require component subject matter expertise.

Red teams. Red teams are actors who seek to replicate the actions of a potential adversary and conduct these actions against friendly forces during an exercise or war game. Red teams allow friendly forces to test their capabilities or plans in order to discover weaknesses or deficiencies in a course of action, tactics or level of competence. The results of a red team interaction allow the rectification of gaps in planning or capability before exposing forces to a real adversary. Organisations that seek to appreciate fully any potential vulnerability use the best players in a particular field to fill the red team, as it should be assumed the enemy would use its best forces in any conflict. The cyber world is no different. The ADF and the RAAF need to develop red teams that seek out weakness in the ADF information systems and exploit them during exercises.[201] Red team cyber operations can be conducted from the joint level, where individual Service cells will enable a focused appreciation of where to focus an attack based on its Service-minded perceptions of potential vulnerabilities. RAAF cyber experts understand what the air component values and needs to conduct air operations. A generically trained cyber operator will lack such an appreciation and not understand where to target or what to defend from a RAAF counterattack.

---

200 United States Joint Chiefs of Staff, Joint Publication 3-30: *Command and Control for Joint Air Operations*, Joint Chiefs of Staff, Washington, DC, 2010, p. III-22.

201 Scott, interview with Squadron Leader Duncan Scott by Squadron Leader Craig Stallard.

RAAF cyber operations and information warfare

Information warfare at the Service level should not include computer network operations in a mature cyber-operations-enabled Air Force.[202] It is a joint function better conducted at the joint/whole-of-government level to support Service needs. Service groups should raise, train and sustain cyber-trained personnel to staff the Joint Cyber Centre (run under the Joint Operations Command with reachback to the Defence Signals Directorate), deployable computer network operations cells for Joint Task Forces, and computer network operations within component operation centres. Each component's cyber operation cells should be integrated into all levels of the component planning organisation, not just a coordination or liaison cell.[203]

No 462 Squadron. The RAAF's Information Operations Squadron has the responsibility for the same elements of tactical computer network operations, with its cyber operations focus mainly on information assurance.[204] RAAF cyber operations are in the developmental phase with a number of projects underway to expand its understanding of how cyber influences Australian air power and provide direction on how best to expand the Air Force's cyber operations. The direction in which the RAAF will develop its future concepts for cyber operations will depend in part on the Commander Joint Operations Command published intent, which is due by the end of 2011, and the subsequent joint concept of operations for the conduct of computer network operations in support of ADF operations. The level of joint versus Service cyber operational capabilities is a subject that is sure to be hotly debated long after the release of the Commander's intent.

RAAF vulnerabilities

To produce its combat effectiveness, the Air Force leverages technology more than any of the other services. Carl Builder describes this phenomenon as worshiping at the altar of technology.[205] Current and emerging military aviation technologies are increasingly reliant on cyberspace to produce combat effectiveness. Thus, the RAAF has a significant interest in securing the cyberspace that underpins its combat capabilities. It will be very difficult to be 'swift, decisive, resilient and

---

202 ibid.

203 Richard Mesic, Myron Hura, Martin C Libicki, Anthony M Packard & Lynn M Scott, *Air Force Cyber Command (Provisional) Decision Support*, RAND Project Air Force, RAND Corporation, Santa Monica, CA, 2010, p. 11.

204 Scott, interview with Squadron Leader Duncan Scott by Squadron Leader Craig Stallard.

205 Carl H Builder, *The Masks of War: American Military Styles in Strategy and Analysis*, A RAND Corporation Research Study, The Johns Hopkins University Press, Baltimore, MD, 1989, p. 19.

respected' if aircraft are grounded or capabilities severely limited due to a lack of access to cyberspace.[206] In cyber terms, the air force has numerous vulnerabilities from a cyber attack that can ground aircraft or reduce their combat effectiveness, which do not involve direct cyber attacks on aircraft. The list of potential RAAF vulnerabilities is long and includes areas such as: sensor fusion and data dissemination for air defence systems; data collection, processing, analysis, and dissemination support for ISR; pre and post-flight cyber support capabilities for aircraft; synchronisation of navigation and weapons; communication infrastructure for data links, satellite communications, phone landlines, video conferencing, secure radios, and the DRN/DSN/DTSN networks; acquisition modelling and processing databases; and computer support activities for research and development activities. For the near future, airborne aircraft are unlikely targets for a cyber attack, but as BH Liddell Hart posits, the indirect approach can be more effective. The following examples of indirect attacks via logistics, maintenance, air defence systems, rules of engagement, and even on the F-35 provide an insight into just some of the vulnerabilities the RAAF must address if it is to continue to rely on cyber as the nerve system for its combat capabilities.

Logistics. Whether domestically or in theatre, the majority of logistic supply occurs through civil contractors, and almost all contractors conduct business over the Internet. Disruption or denial of Internet services can turn off the supply of fuel, spares or rations to an air base. Most logistic systems, including those in the RAAF, use radio frequency identification devices (RFID) to manifest and track items between the supplier and the consignee. These devices and the information systems that support them are enabled by private-sector organisations that use cyberspace defended by public-sourced protection software. An adversary could attack the software and corrupt it to disrupt the logistic system, or devise a macro that reroutes all the RAAF's items to random locations and hides the true locations from the contractor. There may also be a perception that local storage may reduce this risk, but during high-intensity operations, base storage facilities are unlikely to keep up with demands. During Operation *Desert Storm*, a number of Middle Eastern bases required a fuel truck to enter the base every five minutes, 24 hours a day, to keep up with demand.[207] A cyber attack on any part of the civil fuel supply chain could significantly reduce the RAAF's ability to conduct air operations.

Maintenance. An adversary seeking to shape the longer-term operational environment could seek to conduct cyber attacks against maintenance operations. The conduct of aircraft maintenance may be vested in RAAF personnel, but the equipment is supplied and serviced by civilian contractors. An adversary could

206 The RAAF vision statement is: '*One team – swift, decisive, resilient and respected*'.

207 Author's experience during Operation *Desert Storm* deployments.

access the relatively unprotected civil information system and manipulate data to cause equipment to be incorrectly calibrated while seeming correct; just as occurred in the 2010 Iranian Stuxnet worm attack. Imagine the effects on an F/A-18's performance if the engine thrust appears normal but is calibrated low. This may be picked up on the flight line, but the time and effort spent correcting the issue may not be available during a crisis period. Conversely, adversaries can inject viruses into the test equipment that transfer into the aircraft operating systems. These viruses can disrupt the aircraft systems in flight, or they could be a Trojan-Horse-style 'malware' transferring sensitive information back to the adversary whenever the test equipment is hooked back up to the aircraft or sent back to the contractor for servicing. In addition, maintenance documents are increasingly generated in soft copy only. Cyber attacks could corrupt the online manuals or deny the maintainers access to the documents altogether; again significantly influencing the combat effectiveness of air operations.

Air defence. The RAAF values the geographic divide between the Australian northern coastline and countries in South-East Asia as a sufficient buffer to allow an aerial response in the event of an attack. Its prime means of detecting an incoming air attack is an air defence system of radars and other detection options. However, as the former Special Advisor to the U.S. President on Cybersecurity Richard Clarke highlighted, billions of dollars of air defence systems can be made mute by a cyber operation. During Israel's 2008 attack on a suspected Syrian nuclear facility, attacking Israeli aircraft did not appear on the Syrian radars. Though there were formations of aircraft over Syria, no air defence missile was fired, as there were no targets visible on the radar screens to fire at. For the duration of the operation, Israel 'owned' the Syrian air defence system, courtesy of a well-organised cyber operation.[208] Like most modern militaries, the RAAF takes measures to defend its air defence system against cyber attack; however, the lessons from Syria are a stark warning to the consequences of a lapse in CND.

Rules of engagement. The RAAF follows rules of engagement in determining whether a mission can proceed or a particular weapon is authorised for release. A number of these rules are formulated on the collateral-damage assessment for the type of target, the type of weapon, release parameters and identification methods. Behind much of collateral-damage assessment is the fusion of several categories of information, such as intelligence, aircraft weapon characteristics, legal positions and local conditions. In the assessment process, the majority of this information

208 Richard A Clarke & Robert K Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st edition, Ecco, New York, NY, 2010, p. 5.

is stored and processed across cyberspace.[209] A disruption or corruption of any of this data can inhibit the conduct of a mission; even though an aircraft could be overhead the target awaiting clearance. If adversaries can disrupt the collateral-damage assessment process, they can adversely affect the conduct of a mission without even cyber-attacking the aircraft.

F-35 is not immune. The RAAF's next generation fighter, the F-35, will form Australia's foundation for air defence and strike until well beyond 2040. It is truly a wired platform, which enables it to use onboard systems to their maximum effectiveness and integrate off-platform data to generate its aerial superiority. However, does this reliance on networks create vulnerabilities an adversary can exploit? Absolutely, if the RAAF does not develop a cyber force. Central to its maintenance system is the Autonomic Logistics Information System (ALIS).[210] This system enables reports on the status of the F-35's equipment to be automatically transmitted to ground-maintenance units so parts are pre-positioned and maintainers are organised to fix the jet by the time it returns to base. This process can significantly reduce aircraft downtime, allowing rapid turnaround in combat readiness. However, what if an adversary gains cyber access to this system to manipulate the data to read differently from what the onboard problem is? Unserviceabilities would be overlooked, and worse, incorrect actions could delay the platform's return to combat status. A simple over-G error code, inserted into the ALIS, can force days of unrequired corrective maintenance. This is another example of an indirect cyber attack impacting the operational effectiveness of the RAAF combat fleet.

Summary

The Australian Defence Force, like all modern militaries, appreciates that its combat capabilities, its support infrastructure, and nearly every enabling function inexorably rely on cyberspace in some manner or another for their operational characteristics. Cyber is part of the Australian military, and it is here to stay, but whether the military is ready to protect itself from cyber predators, maintain freedom of action within cyberspace, or fully exploit an adversary's cyber vulnerabilities is another thing altogether. The move within the ADF to transform from a series of capable but fragmented, combat elements into a force fighting off a focused and networked joint operational awareness, through

---

209 William A Owens, Kenneth W Dam & Herbert S Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, National Academies Press, Washington, DC, 2009, p. 51.

210 *Defence Industry Daily* staff, 'You can track your F-35s, at ALIS' maintenance hub', *Defence Industry Daily*, 2007, viewed 31 March 2011, <http://www.defenseindustrydaily.com/you-can-track-your-f-35s-at-alis-maintenance-hub-04368/>.

the adaption of Network Centric Warfare, is long anticipated but increases the reliance on cyberspace. The ADF and a number of its allied military partners are closer to developing a mature cyber organisation capable of securing its home-based information systems than it is to establishing a joint cyber organisation or advancing cyber capabilities within the Army, Navy or Air Force.

As the Service that embraces technology more than any other, the Air Force needs to understand the benefits and limitations inherent in cyber operations. Similar to having air superiority as its core combat goal, so too is it seeking to achieve some element of cyber superiority to enable a combat edge over its adversaries in the air and in the decision-making loop. Because cyberspace permeates all warfighting domains, the command and control of cyber operations needs to be joint-focused and joint-led. This does not mean that the RAAF does not have a significant cyber role; in fact, it must build its cyber-trained forces so that the air component has personnel who understand the air perspective when conducting cyber operations; in short, they must be air-minded. Cyber weaponeers developing cyber target packages in support of the air component objectives need an understanding of the essential air elements of any target, and how to focus cyber operations to maximise the air combat capability. Ground and maritime cyber operators will not have the insight required to adequately support an air mission, just as a cyber airmen do not have the experience to know the vulnerabilities of naval capabilities or the specifics of maritime vulnerabilities.[211]

Just as there are numerous opportunities within the cyber realm for the RAAF to develop operational advantages, there are at least as many weaknesses within cyberspace that can turn into vulnerabilities if the ADF and the RAAF fail to develop a robust cyber force. Many of the potential vulnerabilities in areas such as logistics, maintenance, mission support, and command and control do not directly stop aircraft from flying; they do not change physics but, unlike its forefathers, the RAAF relies on more than physics to deliver air power.

To support the defence of Australia through air power, the RAAF needs a broad appreciation of the elements that shape its combat capabilities, and cyber is emerging as one of those core elements. This level of appreciation develops through cognisance of the national strategic security environment and the guidance provided from the national level in the form of the National Security Statement, National Cyber Strategy, and the Defence White Paper. In combination with this guidance there needs to be an understanding of command and control in cyberspace and a sense of the complexity of cyber operations. Only after threading

211 The term *airmen* is a commonly used term to refer to all aviators and is not considered gender-specific in the same regard mankind refers to all humans not just males. The terms *airman* and *airmen* in the RAAF equate to enlisted personnel in USAF.

all these elements together can a direction for the RAAF's future in cyber operations develop.

Chapter 6

The RAAF and Cyberspace

> *New conditions require for solution and new weapons require, for maximum application new and imaginative methods. Wars are never won in the past.*
>
> General Douglas MacArthur[212]

In a perfect world, there would be no requirement for computer network operations (CNO), because in such a Utopia, there also would be no conflict. However, there is no Utopia, and in this real world, the RAAF comes under cyber attack dozens of times a day.[213] Cyber attacks threaten the conduct of Air Force activities, and in future conflicts cyber operations will play a significant role. If the RAAF is to deliver on its responsibility of providing air power in the defence of Australia, it needs to adapt to each new condition it faces. Cyber is one of the most influential conditions the RAAF will face in this decade and into the next. To meet the challenges and opportunities of the cyber domain, new software-based weapons are necessary, innovative approaches to protect information systems are vital, and new means to exploit an adversary's decision cycle are required. Developing a cyber force is not just a good idea, it is an essential task.

---

212 General Douglas MacArthur, 'General Headquarters, South-West Pacific Area, Press Release', 21 September 1943, viewed 23 April 2011, <http://www.ibiblio.org/hyperwar/USA/RptsMacA/I/RptsI-5.html>.

213 Cameron Stewart, 'Hackers make a mockery of government security', *The Australian*, 3 January 2011, viewed 13 April 2011 at news.com.au, <http://www.news.com.au/technology/hackers-make-a-mockery-of-government-security/story-e6frfro0-1225980765432>.

The needs of a cyber force mirror other air power elements in many ways; they embrace equipment, structure and people. The core elements required to support a RAAF cyber force are; access to equipment or cyber capabilities; an organisational structure that supports RAAF, joint and whole-of-government cyber activities; and people with the training and air-minded attitude for cyber. However, like the development of any new capability, to grow and sustain a cyber force will be neither easy nor cheap, and requires the support of the RAAF and ADF executive.

Budget pressure. Growing a new capability will be a challenge, particularly given the Strategic Reform Program and the fiscal constraints placed on all government agencies. However, if the combat capabilities that underpin Australian air power are to be sustained, and opportunities available within cyberspace exploited, then the ADF and the RAAF must elevate the priority of the development of a cyber force. Fiscal pressure may tempt RAAF capability development to establish a cyber force as an add-on capability to an existing unit; however, this would be like trying to place an F-35 flight under a C-130 squadron—the capabilities have certain synergies, but they perform different functions that require specialist organisations to develop these functions. That said, the argument to raise a new force is not always an easy sell to those who control the budget. Nevertheless, the argument is clear and the risk identified by the former Prime Minister in the 2008 National Security Statement. The RAAF needs a cyber force to maintain access to its information systems and exploit an adversary's use of cyberspace to establish decision superiority. Either additional or reallocated funding is required if the RAAF is to deliver air power in a cyber world. What will the money be spent on? That is easy: equipment, organisation and people.

Equipment

Unlike many other RAAF capabilities, equipment for a future RAAF cyber force is likely to be the lowest capital outlay. While there will be a requirement for computers, routers, training devices, deployable cyber capabilities, and an experimentation laboratory, the financial outlay for this equipment is low in comparison to the cost of aircraft or combat enablers such as over-the-horizon radar. In what is almost a first for the RAAF, the bulk of equipment for a core capability will reside outside of its organisation. The Defence Signals Directorate will be the central repository for the majority of the cyber equipment that will perform cyber operations. The RAAF cyber force will reach back to elements within Defence Signals Directorate to conduct the computer network operations activities required for Service functions or in support of joint operations. There will be a requirement to acquire equipment to support a deployed computer

network operations capability, as connectivity with the Defence Signals Directorate can never be fully guaranteed during a crisis. But cyber operations are very equipment-centric, and computer equipment becomes redundant very quickly, so the cost of maintaining advantages in cyberspace will require frequent upgrades to equipment at a rate far greater than the mainstream RAAF.[214] Despite leveraging off the Defence Signals Directorate's cyber equipment, RAAF capability development planners must plan for the relatively high costs associated with the acquisition and then ongoing cost of maintaining leading-edge computer equipment.

Organisation

After equipment, the most common focus in the development of a new capability is the organisational structure. Does the capability need a separate squadron? To which Wing or Group will it belong? What will be the chain of command and liaison? All are fair questions, but the most important question that needs to be addressed when developing a new force is: 'Whom does the capability support?' Second to this question is: 'From what similar capabilities may we draw synergies?' From these questions the answers to most other questions flow. The primary customer is the RAAF. This may seem obvious and simplistic, but it is essential to clearly establish this fact because the primary customer sets the goals for the force and the boundaries of its operations. Cyber operations are inherently joint, but joint operations require the Services to provide domain-related capabilities. Thus, the RAAF cyber force will operate in the joint environment to provide air-minded cyber expertise to the joint fight. It is the role of the RAAF to raise, train and sustain air power for the defence of Australia, thus all elements of air power are developed and maintained in accordance with the RAAF's goals and objectives. These goals and objectives are devolved from tasks and guidance delivered from the Chief of the Defence Force and the Commander of the Joint Operations Command. The RAAF cyber force will support operational and exercise deployments of air power-related cyber capabilities, while being the lead Air Force agency on all raise-train-and-sustain cyber issues.

Non-governmental sectors. As discussed in chapter 4, cyber support to the public and private sectors, along with critical infrastructure, falls under the responsibility of the Attorney-General. Through the Computer Emergency Response Team

---

214 Adam Brate, *Technomanifestos: Visions from the Information Revolutionaries*, Texere, New York, NY, 2002, p. 321. In 1965, Intel co-founder Gordon Moore predicated computer processing power would double every two years, which was later revised to 18 months. This predication has held true and is expected to continue throughout this decade.

(CERT) and the Trusted Information Sharing Network (TISN), cyber activities are conducted to facilitate individual, corporate and owner/operators of information systems security against cyber threats, and provide support in the event of a cyber attack, as indicated in figure 6–1. During periods of cyber activity, these groups are likely to turn to the Cyber Security Operations Centre (CSOC) for advice and action.[215] Through members currently posted to the Defence Signals Directorate, the RAAF has representation in the CSOC.

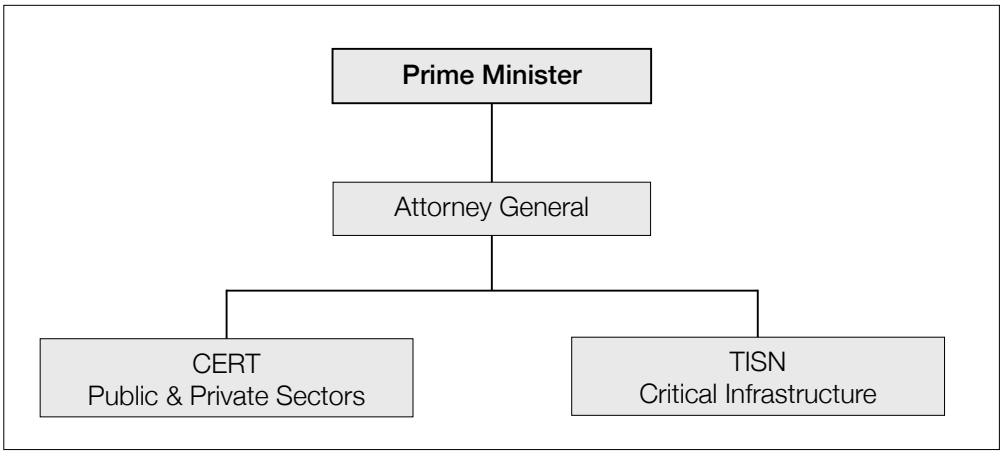

Figure 6–1: Attorney-General responsibility for non-governmental sectors[216]

RAAF computer network operations. To ensure the RAAF's cyber-enabled capabilities continue to deliver air power when required, the RAAF will need to conduct all elements of computer network operations, or have these functions conducted on its behalf. That said, the RAAF has only minimal organic computer network operations capability, thus the responsibility for the conduct of these activities falls to the Defence Signals Directorate. At present, the Directorate has the responsibility to conduct cyber operations to support all governmental departments, including the ADF. While it has been acknowledged through media releases that the Directorate has the responsibility for the defence of government information networks, the majority of work within the Directorate is

215 Defence Signals Directorate, 'The Cyber Security Operations Centre', viewed 13 April 2011, <http://www.dsd.gov.au/infosec/csoc.html>.

216 Source: Author's original work.

classified.[217] However, ministerial-level speeches provide sufficient evidence that the Directorate conducts some form of computer network operations to support military activities.[218]

RAAF and the ADF joint cyber organisation. In current and future ADF operations, the Joint Operations Command, Joint Task Force (JTF), or component headquarters will exercise command and control. The land, maritime and air components will work to support the JTF objectives, with activities tasked through component headquarters. So if the air component seeks to exploit airspace, the maritime component seeks superiority in the seaspace, and the ground component looks to dominate terra firma, then which component will have the lead in the cyber domain? The answer is, it depends. Each component will want its information systems defended to ensure domain-specific capabilities that rely on cyber for combat advantage, or even basic functionality, to remain undisrupted. Equally, components will seek to attack their adversaries within their domain to maximise combat advantage, while pursuing cyber exploitation to provide awareness of the opponent's disposition, capabilities and intelligence. The RAAF's cyber requirements will differ from land, as much as both will differ from maritime. However, in the Australian context, components will not possess the combat capabilities to conduct the full range of cyber operations.

Reachback. Cyber task requests will flow through to the Joint Task Force headquarters, which will synchronise, integrate and prioritise all tasks. However, similar to the components, the Joint Task Force and Joint Operations Command headquarters will not have the capability to perform the cyber operation. All task requests for computer network operations will be channelled through to the Cyber Security Operations Centre (CSOC). The Centre will be tasked in support of the Joint Task Force and perform the required element of the computer network operation. In many ways this arrangement is similar to the conduct of space operations. Neither the Joint Task Force, Joint Operations Command, nor components have space capabilities, but they all seek to use the space domain to enhance or enable their domain-centric capabilities. Reachback is common practice in space; the concept needs to be transferred to cyber operations.

---

217 Attorney-General Robert McClelland, 'Australian Cyber Security Strategy Launched', Attorney-General's Department, 23 November 2009, viewed 13 April 2011, <http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2009_FourthQuarter_23November2009-AustralianCyberSecurityStrategyLaunched?open&query=CSOC>.

218 Senator the Hon. John Faulkner, 'Opening of Cyber Operations Centre', Minister for Defence, viewed 13 April 2011, <http://www.minister.defence.gov.au/FaulknerSpeechtpl.cfm?CurrentId=9883> and <http://www.minister.defence.gov.au/FaulknerTranscripttpl.cfm?CurrentId=9885>.

Deployed CNO capability. The concept of reachback revolves around the ability to maintain communications links and, in the fog and friction of conflict, maintaining uninterrupted or uncorrupted communications cannot be guaranteed. The irony of using reachback to conduct cyber operations is that much of the communication medium relies on cyberspace for its functionality. Thus in a conflict, where cyber is a factor, the Joint Task Force and the components must have local capability to conduct some level of computer network operations. Each deployed location will require a computer network defence capability, with the Joint Task Force maintaining computer network attack and exploitation functionality. These capabilities will be tactical in nature, looking to maintain the integrity of the local information systems for a limited period of time. As part of its raise-train-and-sustain requirement, the RAAF should develop a tactical computer network operations capability for deployment to forward basing and the Air Operations Centre (AOC). So if most of the cyber operations are to be performed at the CSOC, what will be the major role of RAAF cyber elements?

Cyber operational planning team. The RAAF needs to position air-minded cyber specialists at air component headquarters across each level of the warfighting spectrum, and into the domestic support headquarters and centres where cyber planning is conducted. Representation, in the form of cyber operational planning teams (COPTs), will provide an air perspective to the planning of any cyber activity. The size of a COPT would depend on the nature of the task and should be tailored to the scale of the operation. Ideally, the COPT would consist of specialists in each element of computer network operations, familiar with the joint planning and tasking process, capable of liaising with the COPTs of other components and at the Joint Task Force level, and experienced in the cyber support requirements of the particular air power capabilities employed in the campaign.

Air Operations Centre. At the Air Operations Centre, the COPT would form part of the planning teams within the strategy division, combat plans division and combat operations division. COPT personnel will not be a separate team that attends meetings to receive instructions or provide advice; they would be integrated into planning cells in each division. The designation of the COPT as a team indicates they coordinate their planning across all divisions, but they work for the division bosses. They are as essential to the planning process as the weaponeers. If properly integrated, members of the COPT could make cyber more than a force enabler; they could make cyber a force multiplier. If this team is not employed, and cyber is treated as an add-on, at best, air power may lose some of its combat effectiveness—at worst, an adversary could gain cyber advantage and decision superiority.

To gain advantage in cyberspace will require somewhat of a shift in planning mentality. Normally, specialists turn up at an operation familiar with every detail

of the weapons they include in their master attack plans. COPT specialists arrive with an idea of the type of weapons available, but in many cases the weapon may have to be designed to the specific target information system. Because of this need to design on the fly, the time line between target selection and payload insertion may not line up with the air tasking cycle. It is because of these factors that the RAAF needs an air-minded cyber component. A RAAF cyber specialist will understand the types of targets the air component will focus on, the information systems these targets possess, and how a cyber operation could assist the air mission. Additionally, the air-minded cyber specialists would be comfortable with the cyber capabilities required to support the air component combat functions. They would be best placed to advise on the most appropriate means to protect these capabilities from cyber attack or exploitation, or possibly provide advice on how to enhance some of the cyber–enabling capabilities.

Planning starts early. Just as planning for the kinetic and information aspects of a campaign begins well in advance of an operation (at least that is the hope) so too must cyber planning. As time is required to develop a Joint Prioritised Integrated Target List for the kinetic operations of a campaign, so too will the COPT require time to develop a cyber plan to support the targets on the list, or develop separate cyber targets in support of the air component commander's requirements. If the RAAF wishes to exploit certain elements of adversaries' information systems, then lead time is required for the COPT to put together target profiles, develop cyber weapons and possibly deliver cyber weapons onto target systems ahead of the operation. Delivery may require assistance from physical assets or could be conducted remotely; either way preparation time will be required.

RAAF cyber specialists in the JOC. As per the Joint Task Force headquarters, it is in the RAAF's interest to integrate air-minded cyber specialists into the Joint Operations Command (JOC) cyber planning staff. These personnel would not be part of a RAAF COPT integrated into the Joint Operations Command headquarters: rather, they would be air-minded cyber specialists permanently posted into cyber positions on the Joint Operations Command staff. The Joint Operations Command may form its own COPT across the different elements of its headquarters, and the RAAF needs to grow its cyber force to a level where it can sustain the rotation of personnel through the Joint Operations Command. Having Air Force personnel in positions to shape the development of the ADF's cyber policy will be pivotal to the RAAF gaining traction in the fight for budgets, acceptance of cyber as a joint function, and professional growth in its cyber force. *If you can't fight joint, then stay home*, is arguably more applicable to cyber operations than any other capability.

RAAF COPTs in the JTF. Air Force representation in the headquarters of Joint Operations Command and a Joint Task Force has always been essential to provide an air perspective to the campaign plan. With the development of cyber as a combat capability, the air component needs to include the elements of a COPT

into the Joint Task Force headquarters and air-minded cyber specialists into the Joint Operations Command staff. It is envisioned that the Joint Task Force will develop a COPT to augment traditional kinetic and information planning staff. Having air-minded specialists integrated into the Joint Task Force COPT will provide advocacy for cyber-related air operations, as well as a critical conduit between the Air Operations Centre and the CSOC, as depicted in Figure 6–2. Air Force cyber representatives would be instrumental in integrating air component cyber requirements into the master cyber plan and synchronising them with the cyber operations of other components.

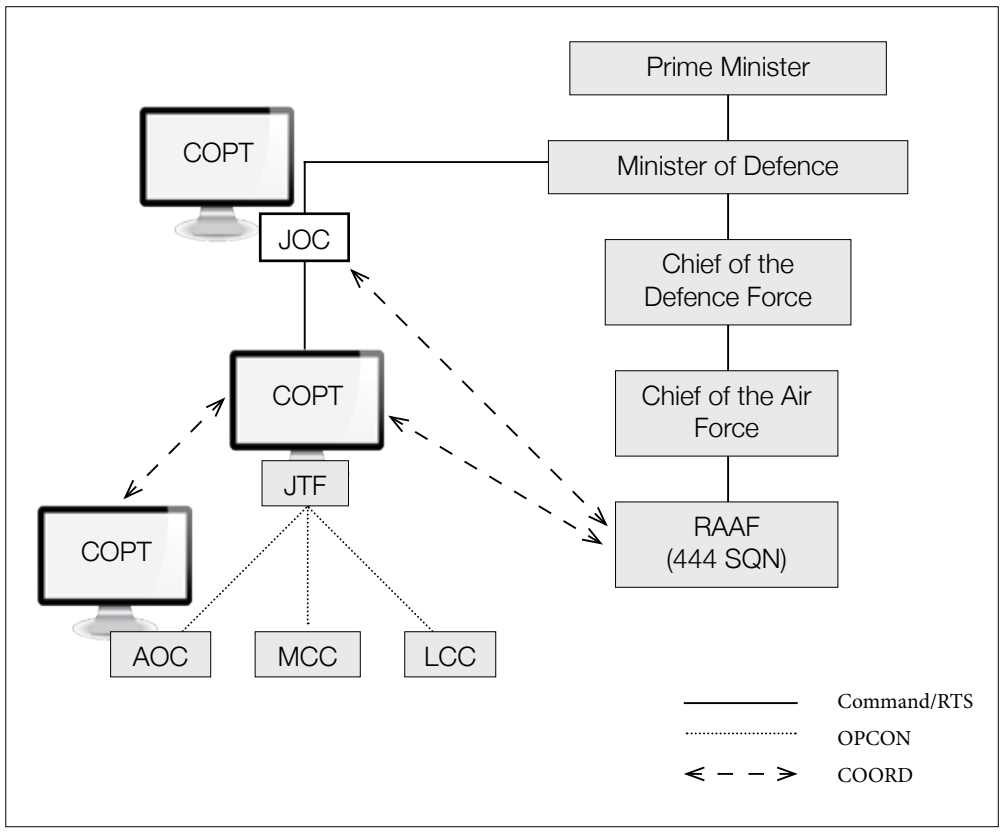

Figure 6–2: Integration of RAAF COPTs into the JTF and AOC[219]

No 444 Squadron – the future of RAAF cyber. The RAAF will not be able grow a cyber force to support the joint fight unless it has a dedicated organisation that

219 Source: Author's original work.

can focus on developing the skill sets required of air-minded cyber specialists. Other cyber experts can expound on the skill requirements of the future cyber warrior, but it is reasonable to argue that the skills will take time to develop and need nurturing though the cyber professional's career. Communications technicians or avionic engineers with a one-month crash course on cyber will not magically become cyber warriors. It will take the training resources and support inherent in a squadron that specialises in cyber. To grow and sustain a cyber force, the RAAF needs a dedicated cyber squadron with a mission focus to raise, train and sustain a cyber force that can support the delivery of air power. Such a unit could be No 444 Squadron.

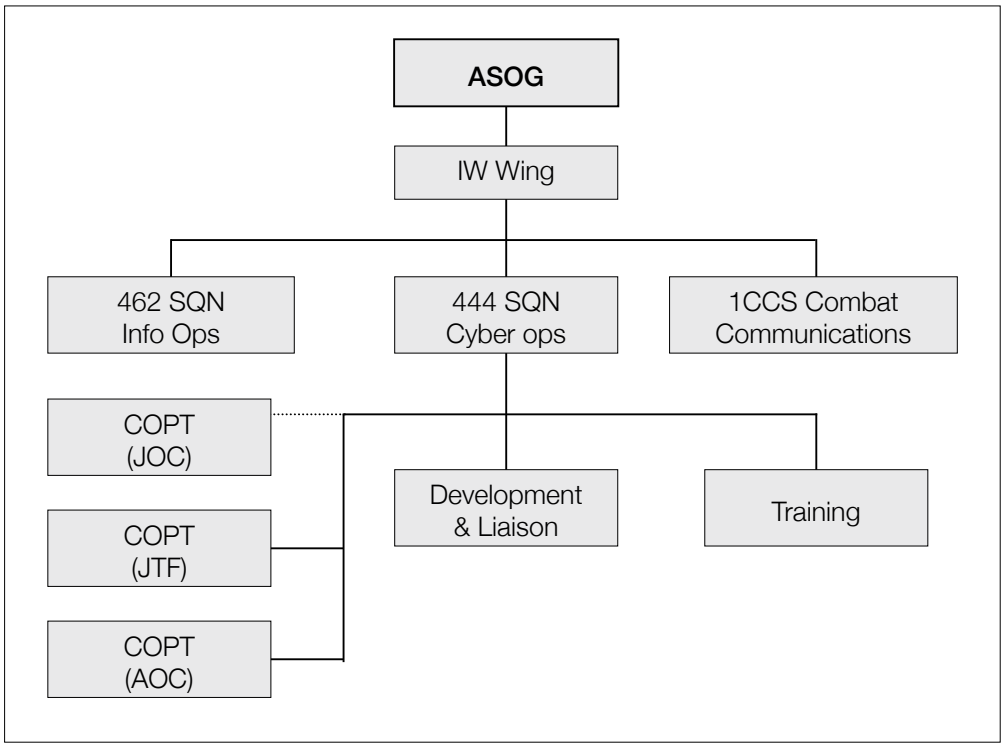

Figure 6–3: Organisational structure for a cyber operations squadron[220]

220 Source: Author's original work.

No 444 Squadron is a fictitious unit, but indicative of a unit established to deliver the cyber needs of the RAAF.[221] The RAAF needs a cyber operations squadron to raise, train and sustain cyber operations personnel capable of deploying as part of a COPT to Joint Operations Command, a Joint Task Force, and an Air Operations Centre, as depicted in Figure 6–3. RAAF cyber specialists would integrate in the Joint Operations Command COPT to provide air-minded perspectives to joint planning, and provide a coordination conduit to the Air Operations Centre to synchronise cyber operations. Air component subject matter experts in the Air Operations Centre's COPT would provide the Joint Force Air Component Commander with air-focused computer network operations options, and synchronise cyber activities across all stages of the air tasking process and planning cycle. In addition, the elements of the COPT would have responsibility for tactical computer network defence of local information systems. The RAAF cyber unit would also grow personnel to support the CSOC and other DSD functions.

This unit is separate from an Information Operations Unit, Intelligence Squadron or a Combat Communications Unit, though there would be a large cross flow of knowledge, and potentially personnel. These units share the cyber domain to undertake many of their functions, but the mission focus and skill sets for each unit differs.[222] The requirement for separate units is analogous to the organisation of flying squadrons. Flying units operate in the same domain, use pilots and other crew members, and operate platforms that share common performance characteristics; Super Hornet, JSF, and F/A-18 classic; C-130 versus P-3C; or C-17, Wedgetail and KC-30. However, each of these platforms and associated squadrons has very different mission sets, its crews are trained to specific platforms, and they approach support to operational objectives through the lenses of different operational functions. Cyber operations are no different; they are just new, and if the RAAF is to gain the advantages it requires from cyberspace and provide the support the Joint Force Commander and Government will expect, then a separate cyber unit is the only real option available, short of a piecemeal approach.

Organisationally, 444 Squadron resembles most other units with operations, training and development flights. Operations Flight manages the COPTs that deploy as part of a Joint Task Force or air component. Those specialists posted into the Joint Operations Command would have an administrative link back to

---

221 No 444 Squadron does not exist and never has existed as a formed unit in the RAAF. The RAAF executive can pick a historical unit or form a new squadron as the unit that provides its cyber needs. No 444 Squadron is used to avoid any political debates on preferences for the re-formation of a disbanded squadron.

222 Squadron Leader Duncan Scott, telephone interview with Squadron Leader Duncan Scott—Executive Officer No 462 Squadron, RAAF Information Operations Squadron—by Squadron Leader Craig Stallard, conducted 3 April 2011, Montgomery, AL, 2011.

444 Squadron for career management and professional training. The Development and Liaison Flight is tasked with keeping RAAF cyber knowledge on the leading edge and nurturing the cross flow of information between the Army and Navy, Joint Operations Command, Defence Signals Directorate and allied cyber organisations. A Training Flight bears the responsibility for initial cyber education, professional development on the cyber field, and developing an air-minded approach to cyber operations.

No 444 Squadron would work in parallel to the RAAF's No 462 Information Squadron and No 1 Combat Communications Squadron. As depicted in Figure 6–3, all three squadrons would report to an Information Warfare (IW) Wing, which would sit under the Aerospace Operational Support Group (AOSG). The computer network operations element currently in 462 Squadron would transfer into 444 Squadron to form the foundation of the cyber force. This organisational structure provides the greatest opportunity for synergistic effect across the RAAF's main units devoted to information-related functions.

People

Equipment and an organisational structure are important elements to the RAAF's cyber force, but people are its most important component. In his 2008 *Commander's Intent*, the Chief of Air Force, Air Marshal Mark Binskin, reiterated, 'people are the key to an effective Air Force.'[223] This is never truer than in the cyber realm, but if people are the RAAF's greatest strength, they also present its greatest challenge. With enough executive support, the RAAF can win a budget war and allocate sufficient funds to train and sustain a cyber force. Air Force can even overcome bureaucratic inertia to stand up a cyber squadron within the RAAF organisation. The real challenge is to raise and train enough of the right people to develop a coherent cyber force, and then retain them in order to sustain a long-term cyber capability. Most members of the RAAF's organisation know and understand computers, but few have the skill sets to undertake general cyber operations, and even a smaller cadre has the ability to plan and conduct air-focused computer network operations. If the Air Force is to develop a cyber

223 Air Marshal Mark Binskin, AM, Chief of Air Force, *Commander's Intent: Air Force: One Team*, Air Power Development Centre, Tuggeranong, 2008, viewed 14 April 2011, <http://www.airforce.gov.au/Leaders/CommandersIntent.pdf>.

capability, it must confront the triad capability endemic to any function: raising, training and sustaining a workforce that does not currently exist.[224]

Raising the Force

Recruitment. Building a mature cyber capability is an enterprise that will take years to realise; there is no droid army of cyber warriors that can be created in short order. However, this does not mean the RAAF has to resign itself to years of cyber wilderness, provided it is committed to the process. By adopting a multifaceted recruiting process that combines entry-level cyber-trained airmen, category transfers, lateral recruiting, and cyber-focused curricula at the Australian Defence Force Academy ADFA), the Air Force should be able to accelerate the cyber skill levels in its new workforce.

Recruit base. A workforce study is required to determine the size of the cyber force; the breakdown of officers, airmen, defence civilians, and civil contractors; the skill sets for each element of the force; and recommendations for sustaining the force. From a RAND study into cyber resource management for the USAF, the best officer candidates for a cyber workforce would come from an electronic warfare or information operations–rated aircrew, cyber-focused intelligence officers, electronic engineers, and communication officers. Even among this pool of officers, the study recommended recruiting from specialised fields inside each category.[225] However, with the RAAF's relatively small force, such a luxury may not be an option, and a more adaptive training program may be required to atone for a broader recruitment base. Ideally, airmen from a communication or intelligence mustering would be the preferred candidates, as cyber-related expertise in these career fields is not uncommon.[226] Similarly, defence civilians with electrical or computer-engineering background, information technology, operational research, or cyber-related intelligence should be the primary focus of a recruiting drive.[227] Ultimately, market availability, the number of appropriately qualified personnel, and the ADF's willingness to transfer troops within a resource-constrained workforce will determine the size of the recruiting pool.

---

224 The RAAF's administrate functions to raise, train and equip in support of its operational role to deliver air power roughly equates to the USAF's responsibilities to organise, train and equip its forces.

225 Lynn M Scott, Raymond E Conley, Richard Mesic, Edward O'Connell & Darren D Medlin, *Human Capital Management for the USAF Cyber Force*, RAND Project Airforce, RAND Corporation, Santa Monica, CA, 2010, p. 19.

226 ibid., p. 21.

227 ibid., p. 22.

Growing a cyber force from the grassroots will take a long time, but if the RAAF is to raise a force with a strong base then, like air and space power, the fundamentals of cyber power must become embedded in the RAAF's entry-level educational institutions. At ADFA, bachelor degree courses in information technology (IT) engineering with computer and information systems majors are on offer; however, less than 10 per cent of the 2010 class have undertaken these majors and none have taken on the IT degree.[228] While a cyber workforce study is yet to be undertaken to establish any type of quota to develop and sustain a cyber force, it is clear a greater number of cyber-skilled personnel will be required. Just as an engineering qualification is essential to underpinning the skill sets required by the engineer branch, so too is a cyber-related qualification core to the maintenance of a cyber force. Equally, the curriculum of the RAAF School of Technical Training can be shaped to provide a greater emphasis on cyber-related education to better inform all RAAF technicians and serve as a lead-in to a cyber-technician course. The recruiting and education of both officer and enlisted personnel for the establishment and sustainment of a RAAF cyber force is not a short-term commitment, and the Air Force will need to seek complementary means to raise a force in the near term.

Lateral recruiting. The RAAF should investigate accelerating its experience base through laterally recruiting serving or recently retired cyber specialists from allied military forces. Over recent years, the United States Air Force (USAF) and the Royal Air Force (RAF) have undertaken substantial growth in the area of cyber operations, developing cyber capabilities beyond the scope of RAAF requirements. Recently separated USAF and RAF cyber operators could provide a kick-start to the RAAF's cyber gene pool, providing a base to develop training and operational knowledge. Additionally, if available uniformed positions are limited, the RAAF should consider developing a cadre of contractors or defence civilians from these overseas organisations. With appropriate remuneration packages, a civilian team could quick-start the establishment of corporate knowledge required to guide the training and development of a cyber workforce.

Skill sets. The cyber workforce, like most military elements, will be comprised of personnel with differing skill sets focused on supporting a common function. This would be analogous to technicians with electrical, mechanical or electronic backgrounds working together to service a single type of aircraft. Therefore, it was not surprising the USAF RAND cyber workforce study recommended a mix of generalist and specialists that would combine to support the cyber fight. 'Generalists', as indicated by the RAND study, 'would have broader experience

228 The ADFA administration department provided the statistics. ADFA is a joint institution that provides military and tertiary academic education for junior officers of the RAAF, Australian Army and Royal Australian Navy.

with the operational application of cyber capabilities; specialists would have expertise with specific information technologies, infrastructures, tools, and codes.'[229] As a small organisation, the RAAF will be better off combining mainstream skills with specific cyber skills. This approach may result in less operational depth across some cyber functions, but in a world of constrained resources, flexibility across a smaller force can be an operational multiplier. The skill sets required to undertake cyber operations in the Air Force environment would be determined by the workforce study on the size, shape and requirements for a RAAF cyber capability. However, the analysis of a workforce study needs to be bounded if it is to be relevant to the RAAF's current and future cyber needs; this framework will be in the form of the Air Force's concept of operations for cyber.

CONOPS. A critical determinate in the development of a cyber workforce is the RAAF's concept of operations (CONOPS) for the conduct of computer network operations. A joint cyber CONOPS will provide guidance on how cyber will support the joint fight, but differing warfighting domains will drive the development of Service CONOPS along domain lines. The realities of resource constraints will place boundaries on the Air Force's conduct of cyber operations, and in many ways these boundaries will shape the character of RAAF computer network operations. A CONOPS will detail how the RAAF will conduct cyber operations, and provide linkages to cyber organisations in the other Services, Joint Operations Command, Defence Signals Directorate, and across international cyber agencies. The CONOPS should presage the recruiting drive, because without a clear framework of what the RAAF wants from cyber operations, a workforce study and recruiting drive would be rudderless. With some resource supplementation, the Cyber and Spectrum Operations Flight within No 462 Squadron would be best placed to develop the Air Force's cyber CONOPS. By being the cradle of cyber knowledge within the Air Force, this flight could splinter off from 462 Squadron and form the nucleus of a separate cyber operations squadron.

Training the Force

Creating a cadre of people with the right aptitude for cyber is only one part of the capability triad; training them to develop an air-minded approach to cyber operations is another essential element. Airmindedness is a state of mind airmen develop though experience and immersion in the Air Force operational environment. It describes how airmen frame issues through the lens of air power. Airmindedness is not created in a classroom, though academic training sets the conditions to understand the application of air power; it must be developed

229 Scott et al., *Human Capital Management for the USAF Cyber Force*, p. 13.

though exposure to the application of air power and derived from experience. To forge an air-minded cyber force, the RAAF needs to balance technical training and education with operational opportunities in order that the cyber cadre perceives issues from an air power perspective. While some of this balance is possible during the initial stages of a member's basic skills and knowledge development, the major element will occur during the formative years in the cyber workforce. The challenge the RAAF faces is how to develop this airmindedness in a cadre that is generally not air power focused.

Shaping the cyber mind. The collective Air Force mind has been shaped by more than 90 years of air power operations, but the cyber mind is relatively infant. To grow the cyber force into one that perceives cyber issues from an air power perspective will require a melding with Air Force corporate knowledge. While this task is challenging it is not impossible; in fact, it happens every day. Across almost every operational capability, the RAAF trains and educates personnel in the art of air power to some degree. Intelligence officers enter the Air Force from a broad range of backgrounds, but normally with little appreciation on how to analyse an air-related issue. Through a series of air-focused courses and employment in positions that immerse them in an air power–related environment, RAAF intelligence officers develop an air-minded perspective. The cultivation of the aircrew mind begins from the very start of initial flying training. Airmindedness is foundational to the nature of the flying trade, but requires continual shaping through operations, exercises and courses to extend the bounds of air perceptiveness. Understanding how to fly a plane is not sufficient to appreciate the most effective ways to apply air power. Equally, being able to conduct basic cyber operations does not translate into being proficient in applying cyber in support of air operations. The same approach to shaping the perceptions of other Air Force operational categories can be adapted to shaping the cyber mind with training, education and operational experience.

Training the cyber mind. Because it operates across all the warfighting domains, cyber is different from other capabilities; thus, training needs to be flexible to meet the specific cyber needs of the RAAF. From the initial course at 444 Squadron, training curricula must include elements of general air power theory and doctrine to raise the awareness of how to apply air power across the spectrum of war. This training includes all aspects of command and control and an introduction to friendly and adversarial combat systems. An in-depth appreciation of the planning for and application of kinetic and non-kinetic weapons is also essential to cyber education. All cyber personnel should undertake a general weaponeering course, similar to that run by the School of Air Warfare. A more specialised weaponeering course, focusing on systems analysis and the application of cyber weapons, will be required as the experience level of a cyber operator increases.

However, while theory is essential, the cyber force needs operational experience to develop its air power mind. From an early stage of their training, members should deploy with air component elements, as well as and other component command centres in order to gain an appreciation of the real-world application of combat power. This will raise the awareness of what the cyber force must defend and provide insights into how component systems can be exploited. Local exercises such as *Talisman Saber*, and international deployments such as *Red Flag*, provide invaluable opportunities to interact with air power operations and to gain insight into the concepts of other friendly-force cyber operations. In the long term, all domestic and international exercises will have cyber elements, and the RAAF must adopt the attitude early that cyber is an integral part of air power—not an add-on to a force package. COPTs must participate in all major exercises.

International connections. The RAAF has a long history of personnel exchanges between international partners as a mechanism to develop broader appreciation of each other's capabilities; this tradition needs to continue within the cyber force. Alongside other air power capabilities, the RAAF should engage with at least the USAF, RAF and Canada in the conduct of cyber operations. The USAF leads all its partners on the development and conduct of cyber, thus, the RAAF should pursue opportunities to engage with elements of 24th Air Force, the Air Force component of US Cyber Command—in particular the 624th Operations Center. As the operational arm of USAF cyber, the 624th plans, directs, coordinates, assesses and provides command and control of cyber operations in support of Air Force and joint warfighting requirements. This exchange would provide 444 Squadron with experienced cyber operators and can accelerate the development of the training program and operational cyber capabilities. The USAF adopted a similar concept with the introduction of the C-17 Globemaster III in order to hasten the capability into service. In addition, the RAF is building its cyber force in response to the growing prevalence of cyber activity. The RAAF should instigate regular information exchange forums between close partners to ensure it remains in step with standards and emerging cyber practices. Exchanges and international conferences are expensive, but if the Air Force is to fast-track its cyber capability, these will be necessary costs.

Developing the cyber mind. More than in any other warfighting domain, changes to operational capabilities occur rapidly within the cyber environment. To pursue advantages in the development of air-focused cyber capabilities, 444 Squadron will require a cyber laboratory as a medium for RAAF cyber operators to conduct air-focused experimentation. Such a laboratory would provide the means for cyber trainees to develop an air-minded approach to their analysis of information systems. A cyber laboratory would be an avenue for experienced Air Force cyber specialists to push through the boundaries of current cyber practices, and to develop innovative air power employment approaches in concert with the Defence Science and Technology Organisation.

Senior leadership. The heart of air power is the workforce that turns equipment into capability, but the brains that turn this capability into operational effect are the senior leadership. Leadership is the product of experience, proven performance and authority without which the RAAF would be unable to deliver the air power expected by the Australian people. Leaders spend inordinate time learning about the capabilities they wield; air superiority, maritime strike, ISR and airlift are but some, to name a few. Unfortunately, there is little experience within RAAF leadership in cyber operations, so if this emerging capability is to be operationally effective, senior leadership will need an education into the realm of cyber. It may take a generation before senior leaders are fully competent in cyber employment; however, tailored cyber courses will allow leaders to take ownership of the cyber capability, as well as develop a foundation for the advocacy of Air Force cyber.

Training the broader RAAF population's cyber mind. Like any new capability, cyber will take a while to gain traction with the general Air Force population. The majority of the RAAF understand the importance of cyber in their everyday lives; there are very few that have not sworn at a computer when it crashes with important data unsaved. The RAAF needs to translate this basic appreciation of computers into an awareness of just how pervasive cyber is to every facet of air power. This can be accomplished in three ways: continuance of the *Pathfinder* series of educational pamphlets on cyber effects on air power, incorporation of cyber elements into every operational training curriculum and, most importantly, introduction of a cyber-disruption component into major exercises. Until the broader Air Force understands the implications of cyber, and develops processes to work in and around cyber disruptions, the ability of the RAAF to sustain air power in an operational environment will be questionable.

Sustaining the Force

Sustaining a cyber force involves ensuring continuity of an operating budget and the maintenance of equipment, but the most crucial element is the sustainment of its people. The Air Force will look to the cyber force to protect its information systems from an adversary and to exploit operational opportunities across the cyber domain. If the RAAF seeks to leverage cyber systems to deliver air power against adversaries, then the management of its cyber force requires a long-term sustainment strategy to retain and promote its personnel.

Raising a new force is a large challenge, but sustaining it over the long term is the critical leg of the capability triad.[230] The development of a cyber force to

230 The capability triad is the raise, train and sustain functions required to maintain a function.

support air operations mirrors the argument of Simon Worden regarding naval forces growing out of a nation's requirement to protect trade and deny trade to its adversaries. An essential need arose and the military developed a solution.[231] But to sustain an emerging workforce is beyond the capability of the operational staff—it requires senior leadership sponsorship. When the US Navy was growing its carrier aviation force, the pushback from regular Navy was so great that, if not for the support from Rear Admiral William Moffett, the effect could have easily collapsed. Admiral Moffett inserted aviators into the Navy promotion system, ensuring the opportunity for command and further progression to star rank.[232] Though different in scale and capability, for the moment, the cyber force requires a personnel management path that meets professional development needs and provides opportunities for career advancement.

Career killer. Chief of Air Force and senior Air Force executive backing is required to ensure RAAF officers view cyber as a career-enhancing specialisation rather than a career killer. A specialist cyber officer should command 444 Squadron. A specialist cyber officer should be made the Officer Commanding of the Information Warfare Wing in the first few years of standing up the capability. Senior Air Force leadership should make it clear that specialist cyber officers will be competitive for the Aerospace Operational Support Group position.[233] Without the possibility of a career path, both the numbers and quality of potential applicants will rapidly drop off and retention will become problematic. The RAAF cyber force could suffer the same fate as the RAN submarine force: resources without the force to operate them.[234] Unfortunately, the loss of an effective RAAF cyber force could have serious negative impacts on the ability to generate air power in the lead-up to and during the period of any conflict.

---

231 Brigadier General Simon P Worden, USAF & Major John E Shaw, USAF, *Whither Space Power?: Forging a Strategy for the New Century*, Air University Press, Maxwell Air Force Base, AL, 2002, p. 100.

232 Stephen Peter Rosen, *Winning the Next War: Innovation and the Modern Military*, Cornell Studies in Security Affairs, Cornell University Press, Ithaca, NY, 1991, p. 77.

233 In the RAAF organisation structure, Wings and subordinate to Groups.

234 Cameron Stewart, 'Joel Fitzgibbon [Minister for Defence] admits "challenge" manning Collins-class submarines', *The Australian*, 25 February 2009, viewed 23 April 2011, <http://www.theaustralian.com.au/news/nation/minister-admits-subs-serious-problem/story-e6frg6nf-1111118958313>; and Attorney-General, *Critical Infrastructure Resilience Strategy*, Attorney-General's Department, Canberra, 2010.

Summary

While the RAAF appreciates the importance of cyber to the conduct of air power, it is still in the early stages of developing a cyber force. Real-time operational pressures, budget constraints, and competition for workforce resources have all contributed to impeding the establishment of a dedicated cyber force. However, the 2009 Defence White Paper has invigorated the Air Force's resolve to raise, train and sustain a cyber force that will support air power through the coming decades. This quest will not be without its challenges, particularly in allocating funds for an operating budget and in the procurement of equipment and subsequent upgrades. Organisationally, the best option for sustaining a cyber force is the standing up of a separate cyber squadron. Such a unit will bear the responsibility for the training and development of the RAAF's cyber elements. Additionally, the cyber unit will provide the nucleus for the Cyber Operational Planning Teams that will integrate into the joint, task force, and air component headquarters' command-and-control centres. The Air Force personnel within the COPTs will provide air-minded cyber perspectives to support joint and component operational planning and coordination.

Budgets and equipment maintenance may occupy much of the RAAF's administrative resources, but it is in the role of raising, training and sustaining its workforce where the real challenges inhere; and cyber will be no exception. From the undergraduate education at ADFA to the Technical Training School, greater emphasis on cyber-related studies is required to provide a cadre of cyber-aware Air Force personnel. However, in the initial stage of building a cyber workforce, the RAAF should seek other options such as lateral-recruiting and exchange programs to accelerate the development of the Air Force corporate-knowledge base. Framing much of the development will be the production of a concept of operations that will establish what the RAAF wants from cyber and how it will undertake these operations. Using this CONOPS, the RAAF should direct a workforce study to provide a roadmap into the size, structure and management practices needed to sustain the cyber workforce. The RAAF is relatively new to operations in the cyber domain, and to grow from its infancy today into a mature capability it will need to both erect and heed the many signposts pointing to its cyber future.

Chapter 7

Conclusion
Signposts for the RAAF

Like many military organisations, the Australian Department of Defence is kinetically focused and structured for the planning and execution of war. Command-and-control practices transformed as the operational environment shifted, and through all the changes the ADF adopted new technologies to retain its position as a leading military power in the South-Pacific region. However, the implications of cyber operations for the ADF and the RAAF run deeper than just a shift in the operational environment. Buoyed by a renewed focus on cyber in the 2009 Defence White Paper, the RAAF is posturing to develop a cyber workforce capable of supporting the delivery of air power during both peace and war. The current level of cyber expertise within the Air Force is low and the path to a functioning, effective cyber force is long and challenging. The journey from present day to a time where cyber operations are seamlessly integrated into every air power capability requires an understanding of what cyberspace is; how it affects command and control; the evolution of Australia's strategic security environment; and where Australia, the ADF and the RAAF are positioned for the conduct of cyber operations. This knowledge informs a general framework for the development of a RAAF cyber capability. This thesis provides insight into some of the required knowledge to develop a cyber force and provides some signposts to guide the RAAF through its cyber journey.

Signposts for the RAAF

- Cyberspace changed both the character of war and the practices of command and control.
- Cyberspace is the 5th dimension of war and is a warfighting domain in its own right.
- Cyberspace permeates all the physical domains of air, land, sea and space.

- Cyber operations do not eliminate uncertainty in conflict but they can diminish it.
- Decision-making time lines for strategic maritime operations are measured in weeks, land in days, air in hours, and space in minutes; but for cyberspace operations, the time line to make a decision could be measured in seconds.
- Cyber provides greater flexibility in the centralisation of control, but commanders need to be cautious with the 5000-mile screwdriver.
- Information is the key to decision-making; cyber operations influence information systems.
- Computer network operations (CNO) are doctrinally part of information operations, but the capability has grown to the extent that it is a function its own right.
- Network Centric Warfare is not cyber operations or Internet-centric warfare, nor is it information warfare; although it utilises elements of all these functions.
- Understanding what national security means to Australia is the first step to understanding how to approach to cyber operations.
- The 2008 National Security Statement provided a framework for the sustainment of the security of Australia's national interests and spawned the 2009 *Cyber Security Strategy* and the 2009 Defence White Paper.
- The northern air-sea gap is not a barrier to cyber operations, as it is to air and sea.
- The Defence Signals Directorate (DSD) bears the responsibility for the security of government information systems and conducts CNO for the ADF.
- With the preponderance of cyber resources, DSD will conduct the majority of cyber operations, including those in support of Joint Task Force and air component objectives.
- Gaining cyber superiority may be a stretch for the ADF, given the nature of cyberspace and the scale of available resources; asymmetric advantage in decision-making gained from cyber is a more realistic expectation.
- The RAAF needs a cyber force to provide air-minded perspectives to the planning and conduct of all cyber operations; this is no different from the approach to kinetic capabilities or intelligence.

- The RAAF is vulnerable to cyber attack today, and given the increasing level of cyber activity, the ability to deliver effective air power is questionable without an air-minded cyber force.
- To appreciate the effect of a cyber attack, all major exercises should incorporate a cyber-disruption component to train the Air Force to continue operating in a degraded cyber environment.
- An Air Force cyber force is essential, but constraints on resources will challenge the RAAF's ability to grow one effectively.
- Within the JTF and Air Operations Centre, Air Force cyber forces should conduct the planning, integration and coordination of cyber operations in support of the air tasking.
- Air Force representation, in the form of cyber operational planning teams (COPTs), will be best placed to provide an air perspective to the planning of any cyber activity.
- The size of a COPT would depend on the nature of the task and should be tailored to the scale of the operation.
- A separate cyber squadron will ensure a single, cyber-focused organisation can develop the skill sets required of air-minded cyber specialists.
- People are the core ingredient to an Air Force cyber capability.
- Raising a cyber force will require a multifaceted approach to recruiting, including category transfers and lateral recruiting.
- Training the force to develop an air-minded approach to cyber operations will not be a short-term process, and it will require specialised air-related courses and experience with all aspects of the air planning and tasking process. The use of COPTs during domestic and international exercises will be essential to developing an air-minded cyber force.
- Training the broader RAAF population is vital to integrating cyber into every aspect of air power.
- Sustaining the force will be the greatest challenge. The cyber force must be able to develop professionally and with career profession opportunities.
- Senior leaders, particularly those who will wield cyber power during operations, must undertake training to appreciate cyber capabilities, as they do for other elements of air power.

If we have learned nothing else from our venture into the cyber realm, we must surely realise that those who seek to exploit our weaknesses for operational

gain are every bit as smart as we are.[235] To be true to its vision of exploiting air power to achieve persistent and precision effects, flexibility, reach, versatility and responsiveness, the RAAF must embrace cyber as core capability and confront the challenges placed in its path. The signposts are out there and need to be followed.

235 Karen Evans & Franklin Reeder, *A Human Crisis in Cybersecurity: Technical Proficiency Matters – A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Center for Strategic & International Studies, Washington, DC, 2010, p. 5.

Bibliography

Alberts, David S, John J Garstka, Richard E Hayes & David A Signori, *Understanding Information Age Warfare*, CCRP Publication Series, Washington, DC, 2001

Alberts, David S & Richard E Hayes, *Power to the Edge: Command…Control… in the Information Age*, Information Age Transformation Series, CCRP Publication Series, Washington, DC, 2003

Allen, Patrick D & Dennis P Gilbert Jr., 'The information sphere domain – increasing understanding and cooperation', Christian Czosseck & Kenneth Geers (eds), *Cryptology and Information Security Series – Volume 3 – The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Press, Amsterdam, 2009

Armistead, Leigh (ed.), *Information Operations: Warfare and the Hard Reality of Soft Power*. 1st edition, Brassey's Issues in Twenty-First Century Warfare, Brassey's, Washington, DC, 2004

Attorney-General, *Critical Infrastructure Resilience Strategy*, Attorney-General's Department, Canberra, 2010

Attorney-General, *Cyber Security Strategy*, Attorney-General's Department, Canberra, 2009

Attorney-General, *Intelligence Services Act 2001*, Office of Legislative Drafting and Publishing, Attoney-General's Department, Canberra, 2001

Attorney-General's Department, 'E-Security', Attorney-General's Departmental website, viewed 27 March 2011, <http://www.ag.gov.au/www/agd/agd.nsf/Page/Nationalsecurity_E-Security>

Binskin, Air Marshal Mark, AM, Chief of Air Force, *Commander's Intent: Air Force: One Team*, Air Power Development Centre, Tuggeranong, 2008, viewed 14 April 2011, <http://www.airforce.gov.au/Leaders/CommandersIntent.pdf>

Blackburn, John & Gary Walters, *Optimising Australia's Response to the Cyber Challenge*, Kokoda Papers No. 14, The Kokoda Foundation, Canberra, 2011

Bousquet, Antoine, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity*, Columbia University Press, New York, NY, 2009

Brate, Adam. *Technomanifestos: Visions from the Information Revolutionaries*, Texere, New York, NY, 2002

Brown, Wing Commander Ralp, interview with Wing Commander Brown—RAF Communications Engineer, UK Ministry of Defence Desk Officer for CNO Policy R&D and Operational Planning 2007–08—conducted by Squadron Leader Craig Stallard, 29 March 2011, Montgomery, AL, 2011

Builder, Carl H, *The Masks of War: American Military Styles in Strategy and Analysis*, A RAND Corporation Research Study, The Johns Hopkins University Press, Baltimore, MD, 1989

Burger, Larry, 'Cyberspace', US Army Strategic Command, Future Warfare Center, Huntsville, AL, 2011

Clarke, Richard A & Robert K Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, 1st edition, Ecco, New York, NY, 2010

Clausewitz, Carl von, Michael Eliot Howard & Peter Paret, *On War*, rev. ed., Princeton University Press, Princeton, NJ, 1984

Convertino, Lieutenant Colonel Sebastian M, Lou Anne DeMattei & Lieutenant Colonel Tammy M Knierim. *Flying and Fighting in Cyberspace*, Maxwell Paper No. 40, Air University Press, Maxwell Air Force Base, AL, 2007

Defence Industry Daily staff, 'You can track your F-35s, at ALIS' maintenance hub', *Defence Industry Daily*, 2007, viewed 31 March 2011, <http://www.defenseindustrydaily.com/you-can-track-your-f-35s-at-alis-maintenance-hub-04368/>

Defence Signals Directorate, 'The Cyber Security Operations Centre', viewed 13 April 2011, <http://www.dsd.gov.au/infosec/csoc.html>

Defence Signals Directorate, 'Cyber Security Operations Centre (Australia)', Department of Defence, Canberra, 2010

Denning, Dorothy E, *Information Warfare and Security*, ACM Press, New York, NY, 1999

Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030 – Defence White Paper 2009*, Department of Defence, Canberra, 2009

Evans, Karen & Franklin Reeder, *A Human Crisis in Cybersecurity: Technical Proficiency Matters – A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Center for Strategic & International Studies, Washington, DC, 2010

Faulkner, Senator the Hon. John, 'Opening of Cyber Operations Centre', Minister for Defence, viewed 13 April 2011, <http://www.minister.defence.gov.

au/FaulknerSpeechtpl.cfm?CurrentId=9883> and <http://www.minister.defence.gov.au/FaulknerTranscripttpl.cfm?CurrentId=9885>

Grant, Rebecca, *Rise of Cyber War*, Mitchell Institute Press, Washington, DC, 2008

Hammond, Grant T, *The Mind of War: John Boyd and American Security*, Smithsonian Institution Press, Washington, DC, 2001

Hastings, Max, *Overlord: D-Day and the Battle for Normandy*, 1st Vintage Books edition,. Vintage Books, New York, NY, 2006

Hinote, Lieutenant Colonel Clint, USAF, *Centralized Control and Decentralized Execution: A Catchphrase in Crisis?*, Research Paper 2009–1, Air University Press, Maxwell Air Force Base, AL, 2009

Houston, Air Marshal Angus, 'Keynote address: the future of air power – RAAF response to the ADF Roadmap', Keith Brent (ed.), *Network Centric Warfare and the Future of Air Power: The Proceedings of a Conference held in Canberra by the Royal Australian Air Force, 16–17 September 2004,* Air Power Development Centre, Tuggeranong, 2004

Hurd, Lieutenant General Joseph E, (USAF, retired), 'Network centric warfare and air power', Keith Brent (ed.), *Network Centric Warfare and the Future of Air Power: The Proceedings of a Conference held in Canberra by the Royal Australian Air Force, 16–17 September 2004*, Air Power Development Centre, Tuggeranong, 2004

Japanese Ministry of Internal Affairs and Communications, 'What Is Bot?', viewed 18 May 2011, <https://www.ccc.go.jp/en_bot/>

Jenkins, Flight Sergeant Karen, telephone interview with Flight Sergeant Jenkins—CNO Supervisor J-5 Effects Cell, Joint Operations Command—conducted by Squadron Leader Craig Stallard, 3 April 2011, Montgomery, AL, 2011

Kenyon, Henry S, 'Cyberspace Command logs in', *SIGNAL Online*, August 2007, viewed 13 March 2011, <http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1362&zoneid=212>

Kometer, Lieutenant Colonel Michael W, USAF, *Command in Air War: Centralized Versus Decentralized Control of Combat Airpower*, Air University Press, Maxwell Air Force Base, AL, 2007

Kuehl, Daniel T, 'From cyberspace to cyberpower: defining the problem', Franklin D Kramer, Stuart H Starr & Larry Wentz (eds), *Cyberpower and National Security*, National Defense University Press and Potomac Books, Washington, DC, 2009

Kugler, Richard L, 'Deterrence of cyber attacks', Franklin D Kramer, Stuart H Starr & Larry K Wentz (eds), *Cyberpower and National Security*, National Defense University Press and Potomac Books, Washington, DC, 2009

Libicki, Martin C, *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, New York, NY, 2007

Libicki, Martin C, *Cyberdeterrence and Cyberwar*, RAND Project Air Force, RAND Corporation, Santa Monica, CA, 2009

Lonsdale, David J, *The Nature of War in the Information Age: Clausewitzian Future*, Cass Series: Strategy and History, Volume 9, Frank Cass, New York, NY, 2004

Luddy, Mr John, *The Challenge and Promise of Network-Centric Warfare*, Lexington Institute, Arlington, VA, 2005

Lynn, Deputy Secretary of Defense William J, 'Remarks on Cyber at the Council on Foreign Relations', Council on Foreign Relations, New York City, NY, 2010, viewed 20 March 2011, <http://www.defense.gov/speeches/speech.aspx?speechid=1509>

MacArthur, General Douglas, 'General Headquarters, South-West Pacific Area, Press Release', 21 September 1943, viewed 23 April 2011, <http://www.ibiblio.org/hyperwar/USA/RptsMacA/I/RptsI-5.html>

MacGibbon, Alastair, 'Cyber security: threats and responses in the information age', Australian Strategic Policy Institute, *Special Report Issue 26*, December 2009, viewed 24 March 2011, <http://www.aspi.org.au/publications/publication_details.aspx?ContentID=233>

Mann III, Colonel Edward C, USAF, *Thunder and Lightning: Desert Storm and the Airpower Debates*, Air University Press, Maxwell Air Force Base, AL, 1995

McClelland, Attorney-General Robert, 'Australian Cyber Security Strategy Launched', Attorney-General's Department, 23 November 2009, viewed 13 April 2011, <http://www.attorneygeneral.gov.au/www/ministers/mcclelland.nsf/Page/MediaReleases_2009_FourthQuarter_23November2009-AustralianCyberSecurityStrategyLaunched?open&query=CSOC>

McNicoll, Air Vice-Marshal Iain, RAF, 'Network centric warfare – perspectives from the United Kingdom', Keith Brent (ed.), *Network Centric Warfare and the Future of Air Power: The Proceedings of a Conference held in Canberra by the Royal Australian Air Force, 16–17 September 2004*, Air Power Development Centre, Tuggeranong, 2004

Merriam-Webster, *Merriam-Webster's Collegiate Dictionary*, 11th ed., Merriam-Webster, Inc., Springfield, MA, 2003

Meserve, Jeanne, 'Mouse Click Could Plunge City into Darkness', CNN online, viewed 6 February 2011, <http://edition.cnn.com/2007/US/09/27/power.at.risk/index.html>. YouTube video of the generator can be accessed at

<http://www.youtube.com/watch?v=fJyWngDco3g>, viewed 6 February 2011

Mesic, Richard, Myron Hura, Martin C Libicki, Anthony M Packard & Lynn M Scott, *Air Force Cyber Command (Provisional) Decision Support*, RAND Project Air Force, RAND Corporation, Santa Monica, CA, 2010

Minister of Public Safety, *Canada's Cyber Security Strategy for a Stronger and More Prosperous Canada*, Ministry of Public Safety, Ottawa, 2010

Mitchell, William 'Billy', *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military*, University of Alabama Press, Tuscaloosa, AL, 2009

Moltke, Helmuth & Daniel J Hughes, *Moltke on the Art of War*, Presidio Press, Novato, CA, 1993

Murray, Williamson & Major General Robert H Scales, Jr., *The Iraq War: A Military History*, Belknap Press of Harvard University Press, Cambridge, MA, 2003

Owens, William A, Kenneth W Dam & Herbert S Lin (eds), *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,* National Academies Press, Washington, DC, 2009

President of the United States, *National Security Strategy – 2010*, Executive Office of the President, Washington, DC, 2010

Reynolds, Colonel Richard T, USAF, *Heart of the Storm: The Genesis of the Air Campaign against Iraq*, Air University Press, Maxwell Air Force Base, AL, 1995

Rosen, Stephen Peter, *Winning the Next War: Innovation and the Modern Military*, Cornell Studies in Security Affairs, Cornell University Press, Ithaca, NY, 1991

Rudd, Prime Minister Kevin, *The First National Security Statement to the Australian Parliament – Address by the Prime Minister of Australia The Hon. Kevin Rudd MP, 4 December 2008*, Department of the Prime Minister and Cabinet, Canberra, 2008, viewed 23 March 2011, <http://www.iseas.edu.sg/aseanstudiescentre/ascdf3_Rudd_NatSec_041209.pdf>

Saalbach, Horst K, *Cyber War: Methods and Practice – Version 3.0*, Universität Osnabrück, Osnabrück, 2011

Scott, Chris, 'Cyber Warfare: A Perspective on Cyber Threats and Technology in the Network-Centric Warfare Battlespace', presentation at US Army Cyber Symposium, September 2008, Information and Systems Technology Group, MIT Lincoln Laboratory, Lincoln, MA, 2008

Scott, Lynn M, Raymond E Conley, Richard Mesic, Edward O'Connell & Darren D Medlin, *Human Capital Management for the USAF Cyber Force*, RAND Project Airforce, Rand Corporation, Santa Monica, CA, 2010

Scott, Squadron Leader Duncan, telephone interview with Squadron Leader Duncan Scott—Executive Officer No 462 Squadron, RAAF Information Operations Squadron—by Squadron Leader Craig Stallard, conducted 3 April 2011, Montgomery, AL, 2011

Sharma, Amit, 'Cyber wars: a paradigm shift from means to ends', Christian Czosseck & Kenneth Geers (eds), *Cryptology and Information Security Series – Volume 3 – The Virtual Battlefield: Perspectives on Cyber Warfare*, IOS Press, Amsterdam, 2009

Smith, Ric, *Report of the Review of Homeland and Border Security: Summary and Conclusions, 4 December 2008*, Government of Australia, Canberra, 2008, viewed 23 March 2011, <http://www.royalcommission.vic.gov.au/getdoc/0be3af5e-16eb-4ba5-93c0-b83cb3a55860/TEN.004.002.0431.pdf>

Stewart, Cameron, 'Hackers make a mockery of government security', *The Australian*, 3 January 2011, viewed 13 April 2011 at news.com.au, <http://www.news.com.au/technology/hackers-make-a-mockery-of-government-security/story-e6frfro0-1225980765432>

Stewart, Cameron,. 'Joel Fitzgibbon [Minister for Defence] admits "challenge" manning Collins-class submarines', *The Australian*, 25 February 2009, viewed 23 April 2011, <http://www.theaustralian.com.au/news/nation/minister-admits-subs-serious-problem/story-e6frg6nf-1111118958313>

Sun Tzu & Samuel B Griffith, *The Illustrated Art of War*, Oxford University Press, New York, NY, 2005

Thomas, Timothy L, *Cyber Silhouettes: Shadows Over Information Operations*, Foreign Military Studies Office (FMSO), Fort Leavenworth, KS, 2005

UK Cabinet Office, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space*, The Stationery Office, London, 2009

United States Air Force, Air Force Doctrine Document 3-12: *Cyberspace Operations*, Department of the Air Force, Washington, DC, 2010

United States Air Force Cyber Command, *Air Force Cyber Command Strategic Vision*, Air Force Cyber Command, Barksdale AFB, LA, 2008

United States Joint Chiefs of Staff, *Capstone Concept for Joint Operations*, Version 2.0, Joint Chiefs of Staff, Department of Defense, Washington, DC, 2005

United States Joint Chiefs of Staff, *Capstone Concept for Joint Operations*, Version 3.0, Joint Chiefs of Staff, Department of Defense, Washington, DC, 2009

United States Joint Chiefs of Staff, Joint Publication 1: *Doctrine for the Armed Forces of the United States*, Joint Chiefs of Staff, Washington, DC, 2007

United States Joint Chiefs of Staff, Joint Publication 1-02: *Department of Defense Dictionary of Military and Associated Terms*, Joint Chiefs of Staff, Washington, DC, 2010

United States Joint Chiefs of Staff, Joint Publication 3-0: *Joint Operations*, Joint Chiefs of Staff, Washington, DC, 2006 (incorporating Change 2, 22 March 2010)

United States Joint Chiefs of Staff, Joint Publication 3-13: *Information Operations*, Joint Chiefs of Staff, Washington, DC, 2006

United States Joint Chiefs of Staff, Joint Publication 3-30: *Command and Control for Joint Air Operations*, Joint Chiefs of Staff, Washington, DC, 2010

United States Joint Chiefs of Staff, Joint Publication 3-60: *Joint Targeting*, Joint Chiefs of Staff, Washington, DC, 2007

United States Joint Chiefs of Staff, *The National Military Strategy for Cyberspace Operations*, redacted edition, Joint Chiefs of Staff, Washington, DC, 2006

United States Joint Chiefs of Staff, *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership*, Joint Chiefs of Staff, Washington, DC, 2011

US Cyber Command. 'U.S. Cyber Command Fact Sheet', 2010, viewed 3 April 2011, <http://www.stratcom.mil/factsheets/Cyber_Command/>

United States Senate, Committtee on Armed Services, 'Nomination of LTG Keith B. Alexander, USA, to be General and Director, National Security Agency/ Commander, US Cyber Command', US Senate, Committtee on Armed Services, Washington, DC, 2010

Van Creveld, Martin, *Command in War*, Harvard University Press, Cambridge, MA, 1985

Waltz, Edward, *Information Warfare: Principles and Operations*, Artech House, Boston, MA, 1998

Waters, Gary, Desmond Ball & Ian Dudgeon, *Australia and Cyber-Warfare*, Canberra Papers on Strategy and Defence, no. 168, ANU E Press, Canberra, 2008

Watts, Sean, 'Combatant status and computer network attack', *Virginia Journal of International Law*, vol. 50, no. 2, 2010

White, Hugh, 'Security, prosperity, and defence', William Maley (ed.), *Australia's Security and Prosperity: Ideas for 2020*, Department of International Relations, College of Asia and the Pacific, Australian National University Canberra, 2008, viewed 23 March 2011, <http://ips.cap.anu.edu.au/ir/pubs/keynotes/documents/Keynotes-9.pdf>

Worden, Brigadier General Simon P, USAF & Major John E Shaw, USAF, *Whither Space Power?: Forging a Strategy for the New Century*, Air University Press, Maxwell Air Force Base, AL, 2002