Australian Defence Force

JOURNAL

ISSUE No. 195, 2014

CONTENTS

CHAIR'S COMMENTS 2

FORTHCOMING SEMINARS AND CONFERENCES 4

ARTICLES

Address by the Chief of the Defence Force 5
Air Chief Marshal Mark Binskin, AC, Chief of the Defence Force

Chinese National Interests and Cyber Capabilities: a 'red team' future 12
Colonel Michael Lehmann, CSC, Australian Army

Rise of the Warrior Geek: the impact of remote systems on future personnel needs 21
Lieutenant Colonel Tim Rutherford, Australian Army

Improving the Australia-India Relationship – A Naval Focus 32
Captain Katherine Richards, CSC, RAN

The Contribution of Submarines to Canada's Freedom of Action on the World Stage 39
Professor Paul T. Mitchell, Canadian Forces College

Improving the Australia-New Zealand Defence Relationship 49
Group Captain Matt Hegarty, Royal Australian Air Force

Challenging the Myths about Flexible Work in the ADF 55
Associate Professor Abby Cathcart, Queensland University of Technology,
Professor Paula McDonald, Queensland University of Technology, and
Dr Deanna Grant-Smith, Queensland University of Technology

East by South-West: the relevance and opportunities for the Australia-Canada security relationship 69
Captain Michele Miller, RAN

The Changing Role of Intelligence within Military Decision-Making 77
Dr Dirk Maclean and
Squadron Leader Charles Vandepeer, Royal Australian Air Force

OPINION PIECE

Energy Competition in the South China Sea: a front-burner issue? 84
Dr Euan Graham, Nanyang Technology University, Singapore

BOOK REVIEWS 87

Chair's comments

Welcome to Issue No. 195 of the *Australian Defence Force Journal*.

We begin this issue with a recent address by the Chief of the Defence Force, Air Chief Marshal Mark Binskin, AC, addressing his vision for the ADF and some of the challenges and opportunities he sees for the ADF in the foreseeable future, particularly in the context of the forthcoming Defence White Paper.

The remainder of the issue features a cross-section of articles on a range of geo-strategic and ADF-related topics, with pleasing contributions from all Services, as well as academics in Australia and overseas, including from our counterpart journal in Canada.

I am pleased to announce that the article by Colonel Michael Lehmann, addressing Chinese cyber capabilities, has been judged the 'best article' in this issue. He will receive a certificate personally signed by the CDF and Secretary of Defence, which is now the standard recognition for winners of this award.

Lieutenant Colonel Tim Rutherford then writes on the 'rise of the warrior geek', arguing that the increased use of remote and cyber platforms will have a dramatic impact on the ADF's approach to training and recruiting. Captain Katherine Richards, one of three contributors currently attending the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies (CDSS) at the Australian Defence College, canvasses a number of naval-related initiatives to further improve Australia-India relations.

We then reprint an article by Professor Paul Mitchell of the Canadian Forces College on Canada's submarine program. While parts of Canada's operating environment are obviously different to Australia's, there are a number of areas of commonality, providing yet another perspective in the context of Australia's future submarine capability. In the following article, Group Captain Matt Hegarty, the second of the CDSS contributors, argues that improved collaboration with New Zealand in strategic air transport would offer Australia greater interoperability with its closest security partner in the South Pacific.

Associate Professor Abby Cathcart and colleagues from the Queensland University of Technology then address some of the myths regarding flexible work arrangements in the ADF, arguing for a broader understanding of flexibility, particularly in relation to hours of work, time-off, changes to duties and location of work. Continuing a mini-theme on our relationship with Canada, Captain Michele Miller—the third CDSS contributor—examines options for closer defence cooperation, both in direct arrangements, such as capability development, and enhanced military engagement to strengthen regional security and build military capacity.

The final article by Dr Dirk Maclean and Squadron Leader Charles Vandepeer addresses the changing nature of 'high-consequence decision-making', particularly in relation to intelligence, surveillance and reconnaissance, outlining also some of the initiatives already being incorporated into a guiding framework aimed at minimising the risk of catastrophic error. We conclude with an opinion piece by Dr Euan Graham of Nanyang Technological University, Singapore on the continuingly topical subject of energy competition in the South China Sea.

Finally, there is a selection of book reviews. As always, we remain keen to hear from readers wishing to join the list of reviewers, who are sent books provided to the Editor by publishers. If you are interested, please provide your contact details and area of interest to the Editor at <publications@defence.adc.edu.au>

The March/April 2015 edition will be a 'general' issue. Contributions should be submitted to the Editor, at the email address above, by mid January. Submission guidelines are on the *Journal* website (see <www.adfjournal.adc.edu.au>).

I hope you enjoy this edition and would encourage your contribution to future issues.

Simone Wilkie, AM
Major General
Commander, Australian Defence College
Chair of the Australian Defence Force Journal Board

Forthcoming seminars and conferences

6-18 October 2015

To be held at the Sydney Exhibition Centre, Glebe Island, Sydney
Sea Power Conference 2015, with the theme 'The Future of Sea Power'
Further details at <http://www.navy.gov.au/spc/news/events/sea-power-conference-2015>

Ongoing

RAAF's Air Power Development Centre runs regular Air Power Seminars
Russell R1 Theatrette
Details at <http://airpower.airforce.gov.au/Home.aspx>

NOTE

To advertise forthcoming seminars and conferences in future issues of the *Journal*, please email details to the Editor
publications@defence.adc.edu.au

Address by the Chief of the Defence Force [1]

Air Chief Marshal Mark Binskin, AC, Chief of the Defence Force

It's a great honour to be the Chief of the Defence Force and to be overseeing the deployment of the ADF to support Australia's national interests around the world. As a G20 nation, Australia is a top 20 economy with a top 15 Defence Force in terms of our size and spending.

We are a Defence Force that has undergone significant modernisation and learning over the past 15 years of high operational tempo. A Defence Force that is highly capable independently, yet also interoperable with the US and a range of likeminded partners both regionally and globally. Our ability to operate effectively with partners in a diverse range of theatres, from Timor-Leste and Solomon Islands to Pakistan, Afghanistan and Iraq, is a stand-out achievement in our recent and current operations. At the same time, we are also in a period of significant cultural reform.

However, if you had told me that during my first five months as CDF that we would have ADF personnel on the ground in Ukraine, be conducting air strikes and deployed a special operations task group to Iraq, be still searching for a missing civilian aircraft in the remote expanse of the Southern Indian Ocean almost 2000 kilometres off the West Australian coast or be monitoring a Russian naval deployment off the east coast of Australia, I would have scoffed at the suggestion.

When I assumed Command of the ADF on the 1st of July, our priority was Australia's ongoing role in Afghanistan; in particular, the 400 ADF personnel deployed in Kandahar and Kabul to train and advise Afghan Security Forces under Operation SLIPPER. We had started to consider our advice to Government regarding Operation HIGHROAD, Australia's enduring contribution to Afghanistan beyond the current ISAF mission, and we had allowed ourselves to begin thinking about the ADF's re-posture following a decade of high operational tempo and multiple overseas deployments. That changed on the 17th of July, 2014 when Malaysian Airlines flight MH-17 was shot down over Ukraine murdering 298 people, 38 of them Australian citizens and residents.

In the days immediately following the crash, the ADF was called to support Operation 'Bring Them Home', Australia's whole-of-government response to the disaster. Our role was primarily to support the Australian Federal Police throughout the Dutch-led operation with an airlift capability. Two RAAF C-17A Globemaster III aircraft led our contribution.

We all saw those sombre images of the Australian aircraft on the tarmac at Eindhoven, as the procession of hearses slowly made their way out of the base. But what you didn't see were the aircrew and ground crew who worked around the clock, loading caskets into the aircraft themselves before transporting the victims from Ukraine to the Netherlands for formal identification and later, returning many of the victims to family and friends in Australia.

Behind the scenes, the mission required extensive planning and cooperation across multiple nations, other Government agencies and time zones. Defence staff in the US, Europe and Australia worked long hours to successfully ensure Australian personnel and equipment moved rapidly into Europe and forward into Ukraine.

Additional RAAF aircrew and aircraft flew support missions between Australia and the Netherlands, while headquarters staff, logisticians, planners, medical specialists, security personnel and other enabling staff in Australia and the Netherlands ensured that those in Ukraine had the resources and back-up required to carry out this difficult task in a complex and dangerous security environment. The current link between the ADF and the Royal Netherlands Defence Force dates back to 2006, when we united in Uruzgan, Afghanistan. That relationship was strengthened as a result of this deployment, while a new association formed with our Ukrainian counterparts.

For me personally, the MH-17 shoot-down highlights three critical points that have set the scene for the tenure of my command:

- the unpredictable nature of the global security environment,
- the complexity of international, inter-agency operations, and
- that the ADF has demonstrated the ability to deploy to the other side of the world at very short notice.

It also demonstrates how much the security environment has changed. Also, increasing globalisation and connectivity has seen Australia's reach and influence grow beyond what has been familiar in the past.

The strategic environment has grown in complexity as increasing economic prosperity fuels the quest for greater military capability from nations that seek to exert power and authority, through to extremist groups that seek the same.

Terrorism, territorial disputes and challenges to sovereignty will continue to demand our attention but the form and nature of these threats is growing harder to predict. Globalisation is allowing extremist groups access to skills, technology and resources that were once difficult for all but state actors to obtain and, consequently, countering terrorism internationally and domestically is one of the most significant challenges facing security agencies around the world—providing insurance against these and other unforeseen challenges that could emerge in the future is one of the ADF's primary functions.

In this environment, I see the ADF as a potent and agile force at the forefront of protecting Australia's security and prosperity. And we work closely with the nation's other security agencies to shape the environment so that we never have to call in that insurance policy. However, as we are seeing, the task of defending Australia and our national interests does not begin and end at our borders. In fact, gone are the days where we focused just on defending the air-sea gap to our north. Today, the interdependence of our nation's security and prosperity with developments around the world mean that the ADF must be thinking and acting regionally and globally as our core business—24/7.

Last month, I met with military leaders from 21 other nations in Washington to discuss the Coalition's fight against ISIL terrorists. Although ISIL has had significant initial success, the Coalition is gaining strategic momentum and partner nations will continue to build on our successes to date. We know ISIL is an adaptive enemy but we have demonstrated that the Coalition has the agility and we have the ability, as partners, to come together to provide the capabilities required to disrupt and degrade their attack.

ISIL has fought to occupy urban centres and relied on road vehicle movement like any conventional force. In the absence of any air power threat, the insurgents were able to advance, but the introduction of a multinational strike campaign has, as predicted, restricted movement and required them to substantially adapt their tactics. The unity manifested in the Coalition to date illustrates our collective resolve to neutralise the ISIL threat and to provide political, economic, humanitarian and military support to the people of Iraq. However, returning stability to Iraq and re-building its security forces will require sustained investment from the international community.

While we must always remain focused on our current operations, we are also at a critical juncture in setting the direction of our Defence strategy, capability and resources. In this respect, the 2015 Defence White Paper will define the shape and capability of the ADF into the second half of this century and provide a coherent, fully-integrated plan for Australia's long-term defence that aligns national interest, strategy, capability, organisation and resources.

One of the most important outcomes from the White Paper will be a long-term affordable plan to build Defence's capabilities to meet Government's strategic aims. This is essential to underpin a strong and sustainable planning basis for the current and future ADF. However, while delivering the White Paper is very important, our success in maintaining the strategy, capability,

organisation and resource alignment over time will be the key test for Government, Defence and the ADF. Being a strategy-led organisation is critical to managing the range of challenges facing us and is requiring us to think differently about some of our decision-making processes.

As you are aware, there are also two associated reviews currently underway which will support the White Paper process. In addition to reviewing our short- and long-term strategic environment, the First Principles Review of Defence will provide a perspective on how we can better achieve and sustain this alignment. Additionally, we are undertaking a Force Structure Review to determine what capabilities Defence requires to meet those challenges, and examining our readiness and sustainability requirements. With these elements combined, the White Paper process is critical to determining Australia's defence future.

Ultimately though, the 2015 Defence White Paper and its decisions are a matter for Government. We are acutely aware that Government expects the White Paper to be founded on a very sound costing basis that gives the Commonwealth confidence that the investment in Defence is sustainable and efficient. In order to do this, we are examining the basis for Defence's cost estimations of our current and potential future capability choices. In addition, to support the Department's development of the White Paper, the Minister appointed an expert panel to provide independent, external advice to the Minister. We are working closely with the panel and meet with them regularly to discuss relevant issues and gain their input.

However, the White Paper does not come with a blank cheque. As CDF, I am cognisant that we must be responsible and accountable with the taxpayers' money and provide a realistic, affordable plan that meets our objectives. The Australian public must be assured that its investment in the ADF is both effective and value for money and be confident that Australia will maintain an ADF that can continue to assure our nation's security in the future.

We must build on our core strengths while introducing new and better capabilities in the joint area, in particular those areas that will be central to success in information and decision superiority in the future. And we must do this while maintaining the integrity of the balanced, integrated and joint force currently at the heart of the ADF that provides great flexibility to move quickly across the spectrum of military operations.

I expect us to be a force that has intelligence, surveillance, infrastructure, ICT, logistics, command and control, and other enablers in place to make the force work when and how we need. I can confidently speak for the Defence leadership group in saying that we understand very clearly the need to ensure that the enablers are front and centre in the decisions about the future force and funding priorities.

Historically, Australia has always been an outward-looking state with regional priorities and global interests. But where we have previously made the geographic distinction between those interests close to home and those in the broader region, particularly Southeast and North Asia, the evolving security environment means we now also look much further afield.

In the interests of promoting global stability, the ADF has deployed to conflicts and humanitarian and disaster relief operations far from our shores. This was the impetus behind the Australian Government's initial decision to employ Australian forces in northern Iraq in mid August to conduct humanitarian air drops to assist the thousands of Yezidi civilians who were driven from their homes and became trapped on Mount Sinjar. In this case, we delivered much-needed bottled water, high-energy biscuits and hygiene packs directly to those in need. This was successful despite the threat that ISIL posed to our aircrew and aircraft.

The follow-on Iraq deployment demonstrates just how far the ADF has come in the 21st century. We have learnt a great deal, both strategically and tactically, from our various overseas operations over the past 15 years. Not just from those high-profile operations in the Middle East region but also on long-term deployments in our own backyard in Timor-Leste and the Solomon Islands, and extremely short notice deployments such as PAKISTAN ASSIST II in 2010, Operation PACIFIC ASSIST in 2011 and, most recently, Operation PHILIPPINES ASSIST in late 2013.

Strategically, strong international engagement by our Defence Force is a significant asset and the future stability and security of our region will depend on our ability to continue to operate transparently and cooperatively with our neighbours.

Tactically, working alongside our coalition allies as a member of ISAF in Afghanistan for the past decade has set a new benchmark for interoperability; importantly, here it is our alliance with the US which affords us access to intelligence capability and high-end technology that boosts our combat power and therefore our overall capability.

Over time, our doctrine, communication, equipment and systems have evolved to new levels of international compatibility. That said, the ADF is more self-sufficient on operations now than we have been at any time in our past. We are no longer 'fitted for but not with' those critical capabilities. Today, we are both fitted for and with the equipment we need to deploy rapidly to conduct humanitarian and disaster relief operations or respond to high-end security threats. Our people are well trained, well equipped and well positioned to make a meaningful contribution. This is true across the entire organisation but if you will allow an old(er) fighter pilot some indulgence, I'll focus on the Air Task Group for a moment.

While a relatively small size overall, the combination of strike aircraft, tankers and airborne early warning and control aircraft mean the Air Task Group currently deployed on Operation OKRA in Iraq is not only one of the most capable air packages Australia has ever deployed, it is also the first completely organic or self-contained Air Task Group we have deployed.

The E7-A Airborne Early Warning and Control aircraft, more commonly known as the Wedgetail, is providing a critical intelligence, surveillance and reconnaissance capability. The Wedgetail is performing two main functions. First is to deconflict and control the tactical battlespace by providing direction to Coalition aircraft. Second is to gather information from a wide range of sources which can be analysed and communicated to air and surface assets. In doing this task, the Wedgetail is proving to be a significant capability multiplier that increases the Coalition's overall effectiveness.

Of course, most of the media reporting has been around the activities being conducted by our Super Hornets. As a multi-role fighter with an advanced air combat capability for air-to-air and air-to-ground missions, the Super Hornet can undertake air interception, close air support and interdiction of enemy supply lines in a single mission. Each Super Hornet mission on Operation OKRA is up to 8-10 hours and each aircraft may refuel up to four times during a single mission, which brings me to the final element of this package—the all important KC-30A Multi Role Tanker Transport aircraft, which is providing refuelling capability not only to the Australian Air Task Group but to other Coalition aircraft including French Rafale, Canadian Hornets and US AV-8B and Hornet aircraft.

Operation OKRA is a significant deployment for the ADF. Our ability to prepare and deploy the Air Task Group and a Special Forces contingent in less than two weeks was a substantial achievement by any military's standards. The ADF's joint warfighting capability is evolving and the forces we can bring to Government to address any contingency reflect this. The ADF possesses a significant capability set that we need to maintain as well as the others we are preparing to bring into service. The first of our two amphibious ships, HMAS *Canberra*, will be commissioned later this month with her sister ship *Adelaide* scheduled for delivery in 2016. And next year, the first RAAF pilots will depart for Pheonix, Arizona to begin learning how to fly the F-35 Joint Strike Fighter. Both these capabilities will be a game changer.

Generating military capabilities is complex, specialised and expensive work. It is important to maintain at least some capabilities to meet high-end threats in order to deter our adversaries and maintain our credibility among the world's militaries. We are seeing growing military capabilities in our own region, which does not necessarily increase the risk of a major conventional attack against Australia but it does mean we need to carefully consider a strategy that balances the risks and opportunities.

As a consequence, we must strengthen our core warfighting capabilities as the foundation for our ability to undertake the full range of roles and other military tasks the ADF must be able to achieve. Wherever the ADF deploys over the next 20 years, we will likely face a more dangerous operating environment. We must be flexible enough and capable enough to respond when Government asks us to do so, wherever Australia’s national interests are engaged across the world. But we must also employ an appropriate posture in our region to help minimise the risk that we will need to employ the ADF in conflict, while maximising our ability to effectively work with a range of partners to meet common security challenges.

As I have alluded to a number of times, we share regional and global interests with many others and therefore we have to focus on building Defence partnerships and international capacity to address these common security challenges. Military and broader Defence engagement and presence in our region is more important than ever. We cannot afford to take our relationships for granted.

Our own future stability and security will depend on a strong international engagement, as well as our ability to operate transparently and cooperatively with our neighbours. This can only be achieved through greater regional engagement.

In the past five months alone, each of the Services has conducted important regional engagement. One of the most significant exercises was recently staged in the Northern Territory. Exercise KOWARI was the first tri-lateral exercise involving Australia, China and the US. This land-based survival training marked an important milestone in Defence cooperation between the three nations and demonstrated a commitment to enhancing mutual trust, cooperation and regional security.

For three weeks in August, Air Force hosted 110 aircraft and 2300 personnel from the US, Singapore, Thailand, the United Arab Emirates, New Zealand and France (New Caledonia) for Exercise PITCH BLACK 2014. Held every two years, PITCH BLACK is our largest, most complex air exercise and this year it was followed by the RAN's largest maritime warfare exercise known as Exercise KAKADU. Over two weeks, more than 1200 naval personnel, eight warships and 26 aircraft from 15 coalition forces throughout the Asia Pacific and Indian Ocean regions conducted tactical warfare planning as well as high-end warfare serials.

Last week, we concluded Operation RENDER SAFE in Bougainville. I cannot overstate the significance of the work our personnel have undertaken over the past four weeks. Our Explosive Ordnance Disposal technicians have found and destroyed more than 2000 World War 2 bombs and items left in the Pacific—over 16 tonnes of unexploded ordnance. This important work reduces the threat to local populations as well as opening up land for civic uses including horticulture.

Back home, Australia hosted around 1150 US Marines over the six months to October, on a rotational deployment to ADF facilities in Darwin. These rotations have become part of the business as usual of the Alliance, and provide increased opportunities for Australian and US forces to train together and to also deepen defence relations with regional countries.

To our north, the recent decision by the Japanese Government to adjust its constitutional interpretation to allow the Japan Self-Defense Force to play a more active role in the region’s security is also welcome. This change to Japan’s policy settings will also allow for deeper defence relations between Australia and Japan, including more sophisticated exercise engagement.

Defence’s programs, activities and presence, including through our in-country Defence and maritime surveillance advisers across the South Pacific and operations across the Indo-Pacific are also critical to a strong, capable and interoperable ADF and sustainable security in our region. They are about building shared understanding and international capacity to address common challenges.

The returns we gain for Australia’s security from these investments far outweighs their cost.

And finally, we should not understate the criticality of our longstanding Defence relationships in the Middle East either, particularly in facilitating our ability to deploy quickly and effectively into that region. I can confidently say that we would not have been able to deploy on Operation OKRA without the trust and goodwill that has been built up over time. This brings home the point again that coalitions are about far more than boots on the ground and that, in the future, we must take a strategic approach to our Defence relationships and presence in key regions.

While the ADF has demonstrated its strengths as an arm of Australia's national power over recent months, our security environment will remain susceptible to rapid change. The ADF must be ahead of the curve if we are to continue to provide the military capability to support Australia's aspirations for its security and prosperity today and over the coming decades.

In closing, I would like to draw on the statement I made to the ADF when I assumed command.

> My intent is for a Defence Force assured of success at all levels of operations; from humanitarian and disaster response through to high-end warfighting. A joint force that can control the air, maritime and land domains along with the associated cyber space in an operation. A joint force that fully understands and uses our enablers to the best effect, including space, intelligence, electronic warfare, acquisition, logistics, IT systems—and, most importantly, how we prepare our people.

My priority over the next four years is to successfully transform the ADF into the next generation force in accordance with the strategic direction of the upcoming 2015 White Paper. We must learn from the successes and failures of our past to ensure that we transition as a capable and professional force that is trusted and respected by all Australians and the region.

In fact, Australians expect—and deserve—no less.

Air Chief Marshal Binskin's service commenced in 1978 with the RAN. On completion of flying training, he was posted to fly A-4G Skyhawk aircraft. In 1982, he was selected as the first RAN pilot to undergo an exchange with the RAAF, flying Mirage III aircraft. On completion of this exchange and with the disbanding of the Navy's fixed wing capability, he joined the RAAF.

Air Chief Marshal Binskin's other flying tours include No 2 Operational Conversion Unit and No 77 Squadron at Williamtown, flying Mirage and F/A-18 aircraft; training on F/A-18 aircraft with the US Navy at Lemoore, California; instructing on F-16C aircraft with the US Air Force at Luke Air Force Base in Arizona; and No 75 Squadron at Tindal, Northern Territory, flying F/A-18 aircraft. His flying qualifications include Fighter Combat Instructor and Tactical Reconnaissance Pilot. Additionally, he has served as the RAAF F/A-18 Hornet Demonstration Pilot. He has over 3,500 hours in single-seat fighter aircraft.

Air Chief Marshal Binskin's command appointments include Commanding Officer of No 77 Squadron at Williamtown, Commander of Air Combat Group and later as Air Commander Australia. He has served in various joint staff positions, including Staff Officer to the Chief of the Defence Force and in the Defence Materiel Organisation as Officer Commanding the Airborne Early Warning and Control System Program Office.

During Australia's 2003 contribution to the war in Iraq, Air Chief Marshal Binskin served as Chief of Staff at Headquarters Australian Theatre. Following this, he served as the Director of the US Central Air Force Combined Air and Space Operations Centre, where he was responsible for the conduct of coalition air operations in support of Operation IRAQI FREEDOM and Operation ENDURING FREEDOM.

Air Chief Marshal Binskin is a graduate of the Harvard Business School's Advanced Management Program, the Australian Institute of Company Directors and RAAF Command and Staff Course, where he was awarded the Chief of Staff's Prize for Professional Excellence. Air Chief Marshal Binskin was Chief of the Air Force from 2008-11, Vice Chief of the Defence Force from 2011-14 and was appointed Chief of the Defence Force on 30 June 2014.

NOTES

1 This is a slightly edited version of an address delivered at a function organised by the Australian Strategic Policy Institute, Canberra on 12 November 2014, available at <https://www.aspi.org.au/events/dinner-with-chief-of-the-defence-force-updated>

Chinese National Interests and Cyber Capabilities: a ‘red team’ future [1]

Colonel Michael Lehmann, CSC, Australian Army

Introduction

The economic, political and military rise of China poses the classic dilemma of how to accommodate an emerging power within an existing international order. In November 2011, President Obama implicitly recognised this dilemma when he welcomed the role that a ‘peaceful and prosperous China’ could play—as long as it met US expectations regarding fair trade, human rights, the rule of law, freedom of navigation, and democratic principles.[2] Underlying this conditional welcome is a US suspicion that China does not share a commitment to those principles and only conforms to international norms when it suits its national interests. US perceptions of Chinese cyber espionage and other activities resonate with this suspicion.

Indeed, cyberspace has become a strategic issue for the US and China. The US is particularly concerned that cyberspace is being used as a vector for economic espionage. General Keith Alexander, formerly the most senior US cyber official, has called the theft of US intellectual property the ‘greatest transfer of wealth in history’, estimating it costs the US economy $250 billion each year.[3] More broadly, a 2012 survey reported that Chinese ‘cyber attacks’ were the most common issue of concern over China for US government officials, retired military officers, business leaders and academic experts.[4]

Such concerns have led to US officials strengthening their language attributing cyber espionage to China. While the Chinese deny these accusations, reports of Chinese cyber attacks on business, defence, media, and human rights organisations are widespread and credible. Perhaps the most notable public evidence is a 2012 report by the cyber security company Mandiant, which identified the People’s Liberation Army (PLA) Unit 61398 as a major Chinese cyber attacker. Mandiant based this assessment on similarities between Unit 61398’s known mission and the victim’s roles; the location of both the attacker and Unit 61398 in Shanghai; a comparison of known Unit 61398 capabilities to the estimated staff and computing resources needed to carry out the detected espionage; and the ability to tie individual hackers to Unit 61398, including ‘Rocy Bird’, a PLA hacker who blogged about his work.[5]

Presumably reflecting classified US knowledge, General Alexander has since said that Mandiant’s findings were ‘just the tip of the iceberg’.[6] While publicly-available evidence of Chinese cyber espionage may not include a ‘smoking cyber gun’, it nonetheless presents a picture of a gun that is government-issue, still warm, and covered in PLA fingerprints. It is little wonder that President Obama raised cyber espionage twice with President Xi Jinping in 2013, or that US frustration led to the May 2014 indictment of five PLA hackers in a US district court for computer fraud, identity theft, economic espionage, and the theft of trade secrets.[7]

So if Chinese cyber espionage is such an issue in its relationship with the US, why does China persist with it? The answer is simple: cyber espionage directly and successfully supports China’s national interests. Firstly, China uses cyber espionage to vacuum up information that assists its economic growth and development, contributing to the legitimacy of the Chinese Communist Party (CCP). Secondly, China employs cyber espionage for national security purposes, particularly to help the PLA modernise. It does so by seeking to steal advanced military technology and research, such as details of Lockheed Martin’s Joint Strike Fighter. Lastly, while not espionage, the CCP uses extensive cyber measures to monitor and control the cyberspace activities of its citizens and foreign critics, targeting undesirable political criticism.

Given this intimate relationship between cyber activities and its national interests, there may be a tendency for China to adopt a business-as-usual approach in the future. However, the strategic

context of China's cyber activities has changed. The economic need for indiscriminate cyber espionage is gone and US attitudes have hardened, tipping towards long-term retaliation. Consequently, the imperative for China is to find a way to better use cyberspace to further its national interests while avoiding the possibility that these activities will become an unacceptable irritant to the US.

Improving China's cyber capabilities: 'disciplining the brain'

When considering how to improve the Chinese cyber 'dragon', the obvious place to begin is the head. Unfortunately for China, the Chinese intelligence apparatus is stove-piped and internally competitive to the extent that it hampers its functionality.[8] The issue begins at the top, where—unlike countries such as the US—China has no mechanism to conduct the whole-of-government functions that would provide it with focused, fused intelligence.[9] This limitation can also be seen in the cyber arena where there is no effective national control or coordination. The PLA's extensive cyber espionage and attack capabilities, for example, are owned by the General Staff Department, which reports directly to the Central Military Commission.

Conversely, the Ministry of Public Security, with its primary responsibility for domestic cyber security, reports to 'the political-legal system' and has representation on the Politburo Standing Committee.[10] To complicate the matter further, independent cyber capabilities are owned by the Army, Navy and Air Force; the Ministry of State Security is active in the information assurance space; the Ministry of Industry and Information Technology has responsibilities for telecommunications and internet security; there are two state bureaus responsible for encryption and classified networks; and there are numerous non-state cyber stakeholders, including academia and Chinese telecommunications infrastructure and cyber service providers.[11]

It is hardly surprising, therefore, that the traditional Chinese mechanisms of 'leading small groups', 'coordination small groups', and state councils have not been able to untangle this web of overlapping cyber authorities and divergent interests.[12] Consequently, the structural inadequacies and inertia of the Chinese intelligence system make it particularly vulnerable to drowning in digital data. While this issue of cross-agency policy coordination may be systemic and its resolution deeply intractable, this does not lessen the imperative for China to review its intelligence arrangements to effectively coordinate intelligence collection requirements and analysis, including cyber activities. Improving China's cyber capabilities first requires China to improve its strategic intelligence governance.

Improving China's cyber capabilities: 'guarding the bloodline'

A fundamental concern for the CCP is ensuring domestic political stability and thereby securing its continued rule. With over half a billion of its citizens using cyberspace in some way, cyberspace has become a 'two-edged keyboard' for the CCP, having the potential to enable China's economic and social future while also threatening to foster and spread anti-government activism. As the Head of the PLA's cyber espionage activities, Major General Liu Xiaobei, has put it 'the internet has a growing power to influence opinion, and has become a new arena and a new platform in our ideological struggle'.[13]

Consequently, China seeks to control cyber activities which may be incompatible with the political interests of the CCP. The basis of this domestic control lies in the pervasive cyber surveillance effort led by the Ministry of Public Security, supported by all levels of government, and involving private companies and paid commentators. China directs similar attention, including conducting actual attacks, against foreign critics of the CCP and its policies, such as human rights groups and Tibetan activists. Despite occasional lapses in control, China's efforts to monitor and control its cyberspace have been remarkably successful, a conclusion consistent with US criticism that Chinese cyberspace is 'one of the world's most restrictive'.[14]

The issue for China is that cyberspace will only grow in importance as China continues to develop and modernise, with the Chinese recognising cyberspace's 'irreplaceable role in accelerating the

development of the national economy, pushing forward scientific and technological advancement, and expediting the informational transformation of social services'.[15] With this growth in interconnectivity, cyberspace poses a threat to the CCP's authority if it allows criticism to be shared and dissidents to organise, disturbing domestic political stability.

Therefore, a balance must be struck between allowing cyberspace to play a positive role in China's economic, political and social future, while preventing cyberspace from becoming a virtual voice of political dissent. Over the next decade, this balance will be an essential part of ensuring domestic political stability and depends on the CCP continuing to effectively minimise unacceptable political activities in, and affecting, China's 'sovereign' cyberspace.

Improving China's cyber capabilities: 'feeding the belly'

The growth of the Chinese economy over the last 30 years has been nothing short of remarkable, lifting over 500 million people out of poverty and creating the world's second biggest economy. In the coming decade, China's economic growth is expected to continue at rates exceeding those of developed countries, while its economy is expected to become the world's largest, or close to it. Cyberspace has played a role in China's economic success by improving economic efficiency and enabling the financial, communications and informational foundations of globalisation.

However, this positive future is not assured and China faces substantial challenges, including fiscal and structural reform, economic inequality, environmental issues, and an ageing population. If these challenges are not successfully addressed, Chinese growth could fall significantly, severely damaging the CCP's economic credentials and political authority. Inkster has suggested that cyber espionage will play an important role in avoiding a low-growth scenario, as it 'offers China an asymmetric advantage which it can be expected to exploit to the full with little concern for the reputational impact'.[16] Inkster is both right and wrong.

There is no reasonable doubt that China is conducting large-scale cyber espionage, focusing on other nations' information technology, government, communications, aerospace and finance sectors.[17] In practical terms, cyber espionage can lead to better products, more efficient manufacturing processes and more competitive prices. It can also assist the Chinese in understanding the marketing, research, decision making and investment strategies of Western competitors. So Inkster is correct in that cyber espionage offers China competitive economic advantage.

Where he is wrong is in concluding that Chinese cyber espionage can continue to operate at the same scale and against the same targets with impunity. This is because a turning point in the debate on cyberspace has been reached. The growing US willingness to attribute cyber espionage to China has given cyber security a public profile that is unlikely to recede. Goaded by public disclosures of Chinese attacks against US government, business, and media over the last two years, there is an emerging US consensus that Chinese cyber activities represent a 'triple threat': to the US economy; to its security; and to its democratic values.

Michael Hayden, the former head of both the National Security Agency and CIA, has said that Chinese cyber espionage has created 'a very uneven playing field', with impacts so serious that the US may have to consider economic retaliation.[18] Additionally, with the US President known to have raised the issue with his Chinese counterpart, and espionage charges laid against PLA members, the issue has become one of US credibility. Somewhat counter-intuitively, even the Snowden leaks may eventually increase the pressure to act against China—if the US is uncomfortable with its own government's cyber intelligence collection, how willing will it be to accept foreign cyber espionage that damages US economic prosperity?

In response, the Chinese may be tempted to predict future US actions on past US responses. This would be a major and unnecessary mistake. With US attitudes hardening, the industrial-scale cyber espionage that has served China so well in the past is becoming a strategic liability. Conversely, China no longer needs to conduct indiscriminate cyber espionage. The strength of China's economy, its significant investment in education and research, and its partnerships with foreign companies and universities give it the potential to compete in most areas.

However, this does not mean that cyber espionage will no longer be in China's national economic interest. Effective cyber espionage will always be in China's interest. However, the need for industrial-scale economic espionage has passed, and the consequences of detection and attribution are becoming strategically disadvantageous. Unfortunately for China, the need to change its cyber espionage policies may be forced upon it, with a US Congressional Committee suggesting a 'long-term and multifaceted approach that centers on changing China's cost-benefit calculus'.[19] The US indictment of PLA hackers is almost certainly nothing more than a first step. Court cases seeking damages, sanctions targeting Chinese firms which have benefited from state cyber espionage, and travel restrictions against individuals are all plausible.

The challenge for China is therefore to change its cyber espionage activities so that their anticipated benefits are justified by their associated risks. This requires China to take two steps. Firstly, it should consciously balance its cyber espionage activities against the risks of detection, attribution and US response. Secondly, it should commence a medium-term restructuring of cyber espionage to move from an industrial-scale approach to only targeting areas where China is not already competitive or when significant national economic interests are at stake. Improving China's cyber espionage capabilities requires it to evolve from the methods that have previously brought success.

Improving China's cyber capabilities: 'sharpening the claws'

The PLA defends China in line with its 'New Historic Missions'.[20] These include promoting national development, which explains the PLA's economic cyber espionage role, and defending Chinese sovereignty, territory and interests. As part of this latter mission, the PLA is modernising so that it has the capabilities necessary to retake Taiwan and, by 2050, become a military peer of the US.[21]

Until these ambitious goals are reached, the Chinese military strategy is one of asymmetric deterrence. This strategy threatens US military strengths, particularly its aircraft carriers, through relatively cheap asymmetric systems, such as fast-attack missile boats, supersonic missiles, and submarines. In this way, if the US was to conduct military action against China, China intends to make the costs prohibitive and any victory pyrrhic.

The PLA's cyber capabilities are a key part of its asymmetric arsenal, contributing to the military capabilities that will allow it to 'win local wars under conditions of informationalisation'.[22] Its cyber espionage activities steal military secrets which accelerate the development of the PLA, while its offensive cyber attack capabilities pose a threat to US command, communications, intelligence and logistics systems. While the US almost certainly remains the world's most advanced cyber combatant, the PLA's cyber capabilities pose 'a genuine risk to US military operations in the event of a conflict'.[23] The PLA's cyber security capabilities are also intended to protect its own critical military information technology from US attack.

Fortunately for the PLA, China is not under US pressure to stop cyber espionage for military gain. This is because national security espionage is regarded by the US as acceptable, while economic espionage is not. Christopher Painter, the US State Department's Coordinator for Cyber Issues, has said that espionage for commercial advantage is 'something that the US doesn't do'.[24] Richard Clarke, a former US National Coordinator for Security, Infrastructure Protection and Counterterrorism, agrees, saying that the US cyber espionage effort targets 'diplomatic (and) military stuff but not commercial competitor stuff'.[25]

From China's perspective, therefore, it has been given a 'hall pass' by the US Administration to continue large-scale cyber espionage activities to steal military technology and support the PLA becoming a peer competitor of the US. In this case, improving Chinese cyber capabilities only requires a continuation of their development path—there is no need for change.

Improving China's cyber capabilities: 'culling the flights'

While China conducts extensive cyber security and espionage activities, the relative sophistication of its cyber tradecraft has been questioned. For example, Mandiant's attribution of cyber espionage to Unit 61398 was partially based on individual lapses in security and a lack of understanding of the trail that their cyber tools were leaving. Examples included PLA hackers using their real identities when setting up accounts later used for espionage; over 600 cases in which technical data allowed hacking activities to be traced back to Shanghai; obvious grammatical mistakes found in malicious code and emails; and individuals advertising their hacking credentials when looking for employment.[26]

The basic nature and extent of these mistakes implies that the Chinese cyber espionage workforce, while large, is not particularly skilled or sophisticated. This conclusion is supported by the US-China Economic and Security Review Commission, which stated in 2012 that Chinese cyber activities mostly involved 'basic and straightforward techniques' but that their sheer volume still made China 'the most threatening actor in cyberspace'.[27] Finally, in contrast to any expectation that China's working-level cyber warriors are elite personnel, there is evidence that China's cyber workforce endures low pay, long hours, isolation and poor leadership.[28]

But if Chinese tradecraft is unsophisticated, then why has its cyber espionage been so successful? Undoubtedly its scale and sheer chutzpah is a factor. But Inkster has claimed that a significant number of China's past cyber successes have also resulted from lax Western attitudes towards security, leading to 'so much fruit which is either low-hanging or windfall'.[29] Northrop Grumman agrees, noting that open-source reports conflate sophistication with success and arguing that compromises are as much the result of insufficient resources or expertise being devoted to cyber security.[30]

While there is no doubt that lax security contributes to cyber espionage success, care must be taken in drawing conclusions based on the lowest common denominator of detected Chinese tradecraft. Such observations are likely to be comforting but misleading, with analysis of three major cyber attacks attributed to China indicating that the tradecraft used was only as sophisticated as necessary to achieve its goals.[31] Additionally, there is significant evidence that the Chinese are capable of sophisticated cyber tradecraft. For example, PLA hackers reportedly compromised the servers of specialist US defence company QinetiQ, 'outmaneuver(ing) QinetiQ's internal security team and at least five companies brought in to help' over a period of three years.[32]

More recently, in September 2013, the computer security company Symantec confirmed the discovery of 'a professional team of [Chinese] attackers with advanced capabilities … who can undertake multiple campaigns at once, breach some of the world's best-protected organizations and can change their tactics quickly to achieve their goal'.[33] Even before Symantec's report, there was evidence that Chinese cyber espionage was becoming more specialised and agile, using different teams (with specific skill-sets) to breach and exploit a target, and altering their behaviour in compromised systems to avoid changing cyber security measures.[34] Finally, Chinese hackers have been reported to be looking towards the future, developing tradecraft to keep pace with emerging cyberspace trends, looking for ways to circumvent two-factor authentication, operate against targets in 'the cloud', and target mobile devices.[35]

These apparent contradictions are not, however, irreconcilable. Ball has suggested that the evidence reflects a Chinese cyber workforce whose 'technical [cyber] expertise is very uneven'.[36] Accepting this conclusion, there are two associated issues for China. First, unsophisticated cyber tradecraft is more likely to be detected and, even more importantly, to be credibly attributed to China. As Chinese cyber espionage is a significant source of tension with the US, it serves China's interests to increase the sophistication of its cyber workforce relative to US cyber security measures. This should reduce the possibility of detection and attribution, simultaneously increasing the chances of ongoing success and reducing tensions.

However, it is unlikely that tradecraft sophistication will reach the point where wholesale cyber stealth is achievable against advanced targets. Consequently, improvements in technical

tradecraft need to be directed by the changes suggested earlier, such as improving strategic governance of China's intelligence system and only attempting cyber espionage where the need justifies the risk. Additionally, unsophisticated tradecraft is unlikely to provide a sufficient skills base to meet the challenges of evolving technology and cyber security measures—the standards of the past will be inadequate to meet the challenges of the future. Consequently, for China's cyber capabilities to remain relevant to its national interests, there should be a multi-agency, long-term effort to significantly improve the technical tradecraft of China's cyber workforce relative to the cyber security of its targets.

Improving China's cyber capabilities: 'avoiding an immune response'

The difficulty of implementing these policies should not be underestimated. Most importantly, the Chinese may not appreciate the need for change. In early 2014, Mandiant reported that the Chinese response to public exposure of its cyber espionage was to temporarily reduce activity and take steps to cover their technical tracks, before resuming their data theft within six months. Mandiant concluded that China 'has no intention of abandoning its cyber campaigns', despite US pressure.[37] Consequently, the changes suggested in this article require a fundamental cultural shift in Chinese intelligence philosophy and practice, as well as a willingness to look beyond parochial organisational interests to consider what is best for China.

Such changes would start when China's cyber stakeholders are convinced of its need. Of particular importance would be support from the PLA and Ministry for Public Security. If these major cyber organisations embrace change, then organisations with smaller remits would have little option but to follow in their wake. In this regard, China is fortunate that Edward Snowden will probably continue to leak details of US intelligence and cyber programs. This offers a unique window of opportunity for China to leverage, shifting the international cyber espionage narrative away from itself and gaining time for change to be considered, agreed on and implemented.

Conclusion

The Chinese state is engaged in industrial-scale cyber activities against both domestic and foreign targets. These activities have successfully contributed to China's national interests by helping grow its economy, protect its sovereignty, and control political dissent. As China's economy and society become more advanced, the importance of cyberspace and state cyber capabilities to its national interests will also increase. The dilemma China faces is that, while successful, its cyber espionage activities have become a powerful irritant in its relationship with the US. Seen by the US as unfair, the irritant of cyber espionage is only likely to become worse, turning into a weeping sore, as the gap between the Chinese and US economic performance narrows. In response, the CCP needs to implement a program of coordinated change to align China's cyber capabilities and activities with future domestic and international challenges.

First, China needs to coordinate its national intelligence effort and its subordinate cyber activities. Second, China should continue to focus on minimising unacceptable political activities in, and affecting, China's 'sovereign' cyberspace. Third, China needs to recognise that the gain-loss calculus for economic cyber espionage is fundamentally changing. The US considers China's economic cyber espionage to be egregious, so it is becoming a strategic liability. To avoid significant damage to its relationship with the US, China should move towards a cyber espionage model which only targets areas where it lags its competitors or when significant economic interests are at stake. In contrast, cyber espionage against military technology targets can continue unabated. Lastly, to increase the effectiveness of its cyber activities in all areas, China needs to take decisive measures to increase the technical skills of its cyber workforce, decreasing the chances of detection and attribution in a constantly evolving cyberspace.

If China does not blindly follow past practices but pro-actively adapts its cyber capabilities and activities, this may result in what Western militaries call the 'most dangerous' course of action. By the end of the coming decade, the West could be faced by a China whose cyber capabilities are coordinated, sophisticated and able to be employed either surgically or *en masse*. To draw an

analogy, this would be a China whose cyber capabilities are as relatively advanced as those of Russia but backed by the might of China's economy and population. A cyber dragon indeed.

Colonel Mick Lehmann has served in a variety of staff, command and operational positions in Australia, overseas and on operations. He is a 2013 graduate of the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College, has three Masters degrees and is currently posted as a project manager in Defence.

DISCLAIMER

The views expressed in this paper are the author's, and do not necessarily reflect the views of the Department of Defence or the Australian Government more broadly.

NOTES

---

[1] This is an updated and edited version of a paper developed by the author while attending the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College in 2013. 'Red team' refers to the practice of viewing a problem from an adversary's or competitor's perspective.

[2] Barack Obama, 'Text of President Obama's Speech to Parliament', *The Sydney Morning Herald*, 17 November 2011, pp. 3 and 5, available at <http://www.smh.com.au/national/text-of-obamas-speech-to-parliament-20111117-1nkcw.html> accessed 26 May 2014.

[3] Josh Rogin, 'NSA Chief: cybercrime constitutes the "greatest transfer of wealth in history"', The Cable blog, 9 July 2012, available at <http://thecable.foreignpolicy.com/posts/2012/07/09/nsa_chief_cybercrime_constitutes_the_greatest_transfer_of_wealth_in_history> accessed 26 May 2014.

[4] Pew Research Center, 'US Public, Experts Differ on China Policies: public deeply concerned about China's economic power', Pew Research Center website, 18 September 2012, p. 15, available at <http://www.pewglobal.org/files/2012/09/US-Public-and-Elite-Report-FINAL-FOR-PRINT-September-18-2012.pdf> accessed 23 May 2014.

[5] Mandiant, 'APT1: Exposing One of China's Cyber Espionage Units', Mandiant website, 19 February 2013, available at <http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf> accessed 26 May 2014; also Barbara Demick, 'China hacker's angst opens a window onto cyber-espionage', *Los Angeles Times*, 12 March 2013, p. 1.

[6] Andrea Shalal-Esa and Deborah Charles, 'Top general says US under constant cyber attack threat', *Reuters* website, 14 May 2013, available at <http://www.reuters.com/article/2013/05/15/us-cyber-summit-alexander-idUSBRE94D12L20130515> accessed 26 May 2014.

[7] See, for example, US Department of Justice, 'US Charges Five Chinese Military Hackers for Cyber Espionage Against US Corporations and a Labor Organization for Commercial Advantage', media release, 19 May 2014, US Department of Justice website, available at <http://www.justice.gov/opa/pr/2014/May/14-ag-528.html> accessed 27 May 2014.

[8] Institute of Global Conflict and Cooperation (ed.), 'China and Cybersecurity: political, economic and strategic dimensions', report from workshops held at the University of California, San Diego, April 2012, p. 2, available at <http://igcc.ucsd.edu/assets/001/503568.pdf> accessed 27 May 2014; also Tobias Feakin, 'Enter the Cyber Dragon: understanding Chinese intelligence agencies', Australian Strategic Policy Institute (ASPI) Special Report, Issue 50, June 2013, pp. 2-3, available at <http://www.aspi.org.au/publications/publication_details.aspx?ContentID=361> accessed 23 May 2014.

[9] Nigel Inkster, 'China in Cyberspace', *Survival: Global Politics and Strategy*, Vol. 52, No. 4, August-September 2010, pp. 54-7.

[10] Peter Mattis, 'The Analytic Challenge of Understanding Chinese Intelligence Services', *Studies in Intelligence*, Vol. 56, No. 3, September 2012, pp. 52-3, available from <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-56-no.-3/pdfs/Mattis_Understanding%20Chinese%20Intel.pdf> accessed 23 May 2014.

[11] Jimmy Goodrich, 'Chinese Civilian Cybersecurity: stakeholders, strategies and policy' in Institute of Global Conflict and Cooperation (ed.), 'China and Cybersecurity', pp. 5-7.

[12] Goodrich, 'Chinese Civilian Cybersecurity', p. 5; Adam Segal, 'Five Trends to Watch for in Chinese Cybersecurity in 2013', Council for Foreign Relations blog, 18 December 2012, available at <http://blogs.cfr.org/asia/2012/12/18/5-trends-to-watch-for-in-chinese-cybersecurity-in-2013> accessed 26 May 2014.

[13] People's Liberation Army, 'Silent Contest' (excerpt translated by Paul McLeod), National Defence University's Centre for Information Control, 26 October 2013, available at <http:///www.youtube.com/watch?v=M_8ISjcoSW8> accessed 23 May 2014.

[14] Freedom House, 'Freedom on the Net 2012', Freedom House website, September 2012, p. 1, available at <http://www.freedomhouse.org/sites/default/files/China%202012.pdf> accessed 26 May 2014.

[15] The Central People's Government of the People's Republic of China, 'The Internet in China', Information Office of the State Council website, June 2010, p. 1, available at <http://english.gov.cn/2010-06/08/content_1622956.htm> accessed 23 May 2014.

[16] Nigel Inkster, 'Chinese Intelligence Operations and Transnational Consequences' in Institute of Global Conflict and Cooperation (ed.), 'China and Cybersecurity', p. 26.

[17] Mandiant, 'APT1', Figure 13, p. 24; also Stephen Doherty, Jozsef Gegeny, Branko Spasojevic and Jonell Baltazar, 'Hidden Lynx – Professional Hackers for Hire', Symantec website, Version 1.0, 17 September 2013, Figure 1, p. 7, available at <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf> accessed 26 May 2014.

[18] Tom Risen, 'Spymaster: US business needs more protection from Chinese hackers', *US News*, 23 October 2013, available at <http://www.usnews.com/news/articles/2013/10/23/spymaster-us-business-needs-more-protection-from-chinese-hackers> accessed 26 May 2014.

[19] US-China Economic and Security Review Commission, *2013 Report to Congress of the US-China Economic and Security Review Commission* (USCC 2013 Annual Report), US Government Printing Office: Washington DC, November 2013, p. 253.

[20] See, for example, 'Hu Jintao urges army to perform "historic missions"', report on NPC and CPPCC sessions, 14 March 2005, available at <http://english.people.com.cn/200503/14/eng20050314_176695.html> accessed 27 May 2014.

[21] US-China Economic and Security Review Commission, *Indigenous Weapons Development in China's Military Modernisation*, US Government Printing Office: Washington DC, 5 April 2012, p. 3; also Jonathan Holslag, 'Trapped Giant: China's military rise', *Adelphi Papers*, Vol. 50, No. 416, 2010, pp. 40-1 and pp. 63-5.

[22] Information Office of the State Council, *The Diversified Employment of China's Armed Forces*, April 2013, p. 3, available at <http://news.xinhuanet.com/english/china/2013-04/16/c_132312681.htm> accessed 22 April 2013.

[23] Bryan Krekel, Patton Adams and George Bakos, 'Occupying the Information High Ground: Chinese capabilities for computer network operations and cyber espionage', Northrop Grumman Corporation: Falls Church, 7 March 2012, p. 10, available at <http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB424/docs/Cyber-066.pdf> accessed 27 May 2014.

24 ‘Interview with Christopher Painter’, *Defense News*, 13 August 2013, available at <http://www.defensenews.com/article/20130813/DEFREG02/308130007/Interview-Christopher-Painter> accessed 23 May 2014.

25 Ron Rosenbaum, ‘Richard Clarke on Who Was Behind the Stuxnet Attack’, *Smithsonian Magazine*, April 2012, p. 2, available at <http://www.smithsonianmag.com/history-archaeology/Richard-Clarke-on-Who-Was-Behind-the-Stuxnet-Attack.html#ixzz240aLlfJX> accessed 26 May 2014.

26 Demick, ‘China hacker’s angst opens a window onto cyber-espionage’; also Mandiant, ‘APT1’, pp. 4 and 38.

27 US-China Economic and Security Review Commission, *2012 Report to Congress of the US-China Economic and Security Review Commission* (USCC 2012 Annual Report), US Government Printing Office: Washington DC, November 2012, p. 9.

28 Demick, ‘China hacker’s angst opens a window onto cyber-espionage’.

29 Inkster, ‘China in Cyberspace’, p. 65.

30 Krekel, Adams and Bakos, ‘Occupying the Information High Ground’, p. 13; also US-China Economic and Security Review Commission, *USCC 2012 Annual Report*, p. 9.

31 These attacks were the so-called Aurora, GhostNet and Shady Rat attacks. See Krekel, Adams and Bakos, ‘Occupying the Information High Ground’, pp. 98-9.

32 Ben Elgin and Michael Riley, ‘China’s Cyberspies Outwit Model for Bond’s Q’, Bloomberg News blog, 2 May 2013, p. 2, available at <http://www.businessweek.com/news/2013-05-01/china-cyberspies-outwitting-u-dot-s-dot-stealing-vital-military-secrets> accessed 23 May 2014.

33 Baltaza *et al*, ‘Hidden Lynx – Professional Hackers for Hire’, p. 3.

34 Krekel, Adams and Bakos, ‘Occupying the Information High Ground’, pp. 100-2.

35 US-China Economic and Security Review Commission, *USCC 2012 Annual Report*, pp. 159-60.

36 Desmond Ball, ‘China’s Cyber Warfare Capabilities’, *Security Challenges*, Vol. 7, No. 2, Winter 2011, p. 81.

37 Mandiant, ‘MTrends 2014 Threat Report’, Mandiant website, 10 April 2014, p. 21, available at <https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf> accessed 27 May 2014.

Rise of the Warrior Geek: the impact of remote systems on future personnel needs

Lieutenant Colonel Tim Rutherford, Australian Army

> History may look back at this period as notable for the simultaneous loss of the state's roughly 400 year-old monopoly over which groups could go to war and humankind's loss of its roughly 5,000 year-old monopoly over who could fight in these wars.
>
> Peter Singer, *Wired for War*, 2009 [1]

Introduction

For over 60 years, Western militaries have engaged in what could perhaps best be described as 'wars of choice'; that is, wars undertaken to preserve national interest as opposed to national sovereignty. While Clausewitz reminds us that war is the quintessential political act,[2] public tolerance for the human cost of wars waged abroad is generally low. The resulting need to minimise the risk that soldiers face has led to a greater emphasis on technologically-based solutions for the achievement of military aims.[3]

This has been exemplified by the popular use of 'drones' during recent conflicts, and the emerging use of the cyber domain in combat. Controlling these systems is a new type of warrior, who is able to generate an effect anywhere in the world without the need to be physically present. Remote warriors, such as drone pilots or cyber operators, leverage technology to fight. However, as technological advances allow war to be fought by more remote means, questions are raised regarding the future of warfare and the types of individuals who will be waging it.

At present, the ADF does not distinguish between remote and traditional operators. Yet military researchers Gregory Conti and David Raymond contend that remote operators have different needs and possess different qualities to the traditional operator, which would suggest that an alternative model needs to be developed to accommodate the changing requirements of soldiering.[4]

The US has sought to address this change through tailored training courses and the creation of a new Cyber Command, although progress has been slow.[5] An increasing demand for remote and cyber-skilled individuals in the private sector is continuing to contest military recruitment strategies, and the prospect of civilianising these roles raises significant legal and ethical issues.[6] So how does the military accommodate the evolving requirements of the remote workforce?

This article will evaluate the proposition that the increased use of remote and cyber platforms will have a dramatic impact on the ADF's approach to training and recruiting methodologies. In doing so, it will explore the increasing importance of remote operations in Western military operations, before examining some of the issues related to current training and recruitment approaches. It will conclude by discussing the extent to which remote and cyber personnel will form the future of the ADF.

Some issues of definition

Before proceeding, it is important to clarify two issues regarding nomenclature and scope. First, as the scale and use of unmanned systems has grown, there has been a corresponding increase in the number of terms used to define the expanding variety of platforms. Quasi-descriptive titles, such as unmanned aerial vehicle (UAV), unmanned aerial system (UAS), tactical unmanned aerial vehicle (TUAV) and unmanned combat aerial vehicle (UCAV) are now routinely used to describe unmanned aerial technology. However, to simplify naming conventions, the default term used for

all unmanned aerial platforms in this article will be remotely piloted aircraft (RPA), which has similarly been adopted by the US Air Force.[7]

Second, a key distinguishing feature between smaller 'tactical' RPA and the larger 'operational/strategic' varieties is the system used to provide the downlink. The use of UHF radio to provide the downlink on smaller platforms limits their operating range to a few kilometres of the ground control station, typically housing the pilot, sensor operator and data analyst.[8] However, the use of satellite communications on larger systems removes this limitation and introduces a new perspective on how wars may be fought 'remotely', challenging the current views on the recruitment and training of their operators. Unless specified, the focus of this article will be on these larger systems.

Rise of the 'warrior geek'

The ADF signalled its first major steps in the use of RPA in the 2009 *Defence White Paper*.[9] In addition to formalising their use for tactical and strategic intelligence, surveillance and reconnaissance (ISR), the White Paper also outlined the ADF's intent to acquire seven large RPA to 'supplement' maritime patrol aircraft.[10] Of note, however, this acquisition corresponds precisely with the reduction in the number of manned platforms scheduled for purchase under the ADF's Project AIR 7000, the replacement of the maritime ISR capability,[11] suggesting RPA are seen as a viable alternative to manned systems.

At the heart of the shift in attitude has been increased recognition of the safety and reliability of RPA. In the past two years, several major US studies have concluded that RPA have a mishap rate comparable to other aircraft fleets at a similar point in their life cycle.[12] These reports contribute to a growing body of work that is raising the profile of unmanned platforms within the broader military environment. RPA are now considered as suitable platforms for a range of tasks beyond their traditional ISR functions, such as command, control, communications and intelligence (C3I) relays and armed strike missions.[13]

Yet the real proof of the shift towards RPA can be found in the money. While budgets for both the ADF and US armed forces have been on a downward trend since the global financial crisis of 2009, spending on unmanned systems in the ADF has been sustained over the same period, with one analyst estimating the Australia had spent $100 million per year over the past five years.[14] In the US, spending on RPA has doubled since 2008 to US$4.2 billion per year,[15] indicating that in an era of capability cut-backs and project deferrals, the unmanned area has been relatively well preserved.

More recently, Australia's 2013 *Defence White Paper* has made further inroads for the 'warrior geek' in the cyber domain, outlining the intent to invest in a comprehensive range of new and expanding capabilities.[16] While the sensitive nature of cyber operations has precluded the public disclosure of what many of these new and expanding capabilities might be, the creation of a Cyber Security Operations Centre within the Australian Signals Directorate has conveyed the ADF's long-term vision for growth in this area. To date, 130 new staff positions have been created and approximately $1 billion in new capital equipment acquisitions are planned.[17]

A more pronounced development in the rising profile of cyber operations has been the establishment of US Cyber Command. In much the same manner as Australia's version, it aims to coordinate existing resources and synchronise warfighting effects to defend the information security environment.[18] While currently a sub-division of US Strategic Command, there are plans to elevate it to independent combatant status in the near future,[19] which would affirm the cyber domain as an operational environment, comparable with US operational theatres in the Middle East and Africa.

Yet the ability for remote operators to work from benign environments raises questions about the skills they need, particularly in an era of constrained budgets. Specifically, is the ADF wasting money by training remote operators to survive in an operational theatre they may never go to?

The need for traditional field skills

Currently, the ADF trains personnel in two phases: common recruit training, where personnel are taught general military skills; and trade specific training, where individuals learn the skills they require to fulfil their role. A recent tri-Service review of the skills taught in ADF-wide recruit training highlighted a focus on physical training, weapon handling, first aid and drill.[20] However, military researchers Gregory Conti and John Surdu contend that while these skills are an important asset in traditional forms of warfare, they have little relevance to the demands of remote warfare.[21]

The uniqueness of the remote operating environment stems from the absence of physical danger to the individual operator. His or her ability to wage war from benign environments, far removed from the battlefield, makes the field skills currently taught in recruit training largely redundant. However, the lack of historical experience in remote operations has made the task of preparing operators with the relevant skills difficult. Given the lack of established alternatives within the ADF, it may be of assistance to review how this challenge is being overcome elsewhere.

The US Air Force, as the functional command responsible for the largest number of remote operators in the US Armed Forces, has been trialling a number of initiatives. One is an 'Undergraduate RPA Training' course. It is a modified pilot's course, conducted over 22 weeks, and entails less actual flying (although candidates must still meet civil aviation authority standards for air crew).[22] It focuses more on the specific requirements of the remote domain, including training in sensor and electro-optical theory, radar and a tailored physiology class to provide students with techniques for remaining alert for 12-hour shifts in a ground control station. While the program appears to have succeeded in providing a tailored training experience for remote operators, there is currently insufficient data to validate the course's aims.[23]

More broadly, it would seem that advances in RPA-specific training have not been matched by training advances in the cyber domain. Despite the highly complex nature of cyber operations, the less regulated nature of the domain has meant formal qualifications have not been regarded as a prerequisite for employment, especially within the realm of cyber security.[24] Information technology commentators Karen Evans and Franklin Reeder made the interesting comparison that 'cyber security is similar to 19th century medicine—a growing field dealing with real threats with lots of self-taught practitioners, only some of whom know what they are doing'.[25]

As the ADF seeks to develop a cadre of cyber operators, it will be obliged to formalise training standards in order to ensure a consistent level of capability. Although the US Air Force is yet to solve this dilemma, one proposal under consideration is for an alternative training regime focused on functional skills relevant to cyber organisations and their capabilities, as well as the fundamentals of communication and information systems.[26] Emphasising the growing importance of information systems as tools of war, its proponent advocates offensive training in targeting and mission planning in order to effectively disrupt, deny or alter transmission systems or industrial control systems.[27]

One contended flaw with this approach is the lack of military conditioning provided to the remote operator. Conti and Surdu note the enduring relevance of values such as integrity, teamwork, dedication to mission, the ability to keep secrets, and creative problem-solving under pressure, which would usually be inculcated during recruit and follow-on specialist training.[28] Without this military foundation, some would argue that the training of a remote operator could be likened to training a civilian workforce to fulfil a military role. But as the remote warrior is not required to deploy into an operational theatre, does the operator need to be military or can the function be performed by a civilian?

The idea of a civilian cyber cadre has many advantages. First, it bypasses the issue of physical bias with enlistment standards; second, it provides more flexibility on how training is conducted; and third, it facilitates greater stability in role, which prevents skill atrophy.[29] However, the legal use of civilian employees as remote combatants is dubious, as noted by Chris Hanna:

> The positioning of a 'warfighting' function within a civilian element raises questions regarding the legal propriety of such action under the … [laws of armed conflict]. If civilians take a 'direct part in hostilities', then they lose their immunity from attack and possibly expose themselves to criminal prosecution.[30]

Many aspects of international law in relation to 'remote warfare' are still in their infancy, and therefore contestable. However, a legal dispute on this issue would put Australia in an interesting ethical bind. Particularly given the trend of conflicts involving non-state actors who continue to challenge the legal distinction between civilians and combatants, any use by Australia of civilians in a combat role may invite allegations of hypocrisy.[31]

Noting these legal and ethical concerns, it is unlikely that a civilian cadre could assume the full spectrum of tasks required of the remote operator, signalling the need for a fundamentally different approach. Such an approach has been described by Lieutenant General David Deptula (US Air Force) as 'projecting power without projecting vulnerability',[32] suggesting a different, less robust kind of warrior is now needed to fight on behalf of the state. So who are these warriors and how does the ADF attract them?

Recruiting a different kind of warrior

From the outset, it is important to note that the rapid growth of remotely-operated and cyber systems has exposed a weakness in recruitment methods. In workforce capability terms, recruitment fuses the two broad components of demand and supply. Traditionally, militaries have sought physically robust, team-oriented and socially astute personnel to develop into skilled teams of proximal operators. Consequently, recruitment strategies have emphasised adventure, comradeship and patriotism to meet that demand.[33]

But this approach is failing to attract the type of person suitable for operations in the remote and cyber environments. In an address to the US Senate in May 2012, the then head of US Cyber Command, General Keith Alexander, declared 'we are critically short of the skills and the skilled people we require to manage our networks and protect US interests in cyberspace'.[34] This shortage within the US Department of Defense is reportedly as high as 90 per cent of the required workforce.[35] If this figure is even remotely accurate, the scale of the shortfall would indicate that a more systemic problem exists within the cyber operations labour market.

For several years, the technology industry has been commenting on the global shortage of trained cyber security personnel. A key factor is the significant rise in on-line business which, over the past five years, has experienced unprecedented levels of theft and disruption through denial of service attacks. A study in 2011 reported a 250 per cent increase in malicious or criminal attacks over the period of the study.[36] The high volumes of personal and financial information now vulnerable to such attacks, and the need to develop credible defences, has resulted in a demand for cyber security skills—in both the private and public sectors—which is outpacing supply.

Dealing with a lack of supply is a relatively new issue for military recruitment. Over the past decade, the ADF has achieved 84 per cent of its enlistment targets and, while there have always been critical shortages in certain trades within the ADF, the principal cause has tended to be retention rather than recruitment.[37] In order to adapt to this situation, the ADF needs to critically review its approach to recruiting this new and different kind of warrior.

Unlike traditional 'proximal' operators, the warrior geek is unlikely ever to serve in a field environment and may not, therefore, respond to the types of active, social or patriotic themes present in most recruiting campaigns. Conti and Raymond observe that cyber operators generally possess qualities such as high technical aptitude, creative problem-solving and a 'hacker' mindset that enjoys manipulating complex systems in ways often unintended by their designers.[38] Their motivations are more likely to revolve around access to leading-edge technology, and the opportunity to confront multi-dimensional problems or learn advanced techniques for dealing with malware.[39]

The issue for Defence is that these qualities do not generally reside in people with a conventional approach to following rules or respecting authority. As a result, they are usually missed by the narrow parameters of the Defence recruiting profile. Altering the ADF's approach to recruitment to more closely reflect the needs of the job would enable a greater portion of the limited cyber workforce to be accessed. Three areas that could be reconsidered are physical standards, criminal history and more flexible remuneration arrangements.

Physical standards

The warrior geek has little need for physical prowess. Success in remote and cyber operations is the product of mental and technical ability, rather than the ability to march long distances or endure multiple G-forces during traditional air combat manoeuvres. In a review of over ten reports into the knowledge, skills, abilities and other characteristics required of RPA operators, not one identified the need for physical mobility.[40] Hence, benchmarking entry standards against physical competence unnecessarily discriminates against the warrior geek demographic.[41]

While it is accepted that a basic standard of physical fitness supports good general health and improved cognitive function, research in this area suggests the advantages are modest at best. Psychologists Oscar Garcia and Silvia Burgos have noted that most studies promoting a strong correlation between physical activity and improved cognitive ability focus on the elderly.[42] When the sample group isolates working-aged adults (18-53), any link is far less discernible.[43] The lack of significant impact that a lower physical standard may have on cognitive function supports the view that this enlistment criteria could be amended without detriment.[44] One suggestion may be to create a 'non-deployable' category of the ADF, specifically for remote operators (although it could have added benefit for others by addressing one of the chronic reasons that people leave the ADF, which is separation from family).[45]

Criminal history

The second area which could be reconsidered relates to criminal history. A recognised quality of the cyber operator is a 'hacking mindset' which, in many cases, has led to illegal acts as individuals have sought to test their skills by gaining access to protected sites within cyberspace. In 2012, the US Navy Postgraduate School's most senior cyber analyst, Professor John Arquilla, contended that denying access to this level of ability is a huge waste of human capital, likening such individuals to 'the rangers of the cyber sphere'.[46]

Advancing Arquilla's belief, others have developed the so-called 'three hats taxonomy' to distinguish the degree of criminality and level of trustworthiness between hackers, where the three hats—white, grey and black—represent an increasing degree of 'malintent'.[47] Of note, the grey hats are 'usually reformed black hats now working as security experts and consultants'.[48] While this taxonomy is of little use to recruiters, it does provide greater clarity on the rationale for illegal acts perpetrated by hackers and suggests that some can be reformed. It is acknowledged, of course, that any such reconsideration of criminal history within the ADF's recruitment process would increase the burden on security vetting agencies and likely necessitate a commensurate increase in funding.

Remuneration arrangements

The third potential area for review is the flexibility and competitiveness of current remuneration arrangements. As market forces increase base salaries for critical trades in the private sector, a method of providing a more responsive pay structure for critical trades within the ADF could be beneficial. The current system of 18-month rolling reviews, undertaken by the Defence Force Remuneration Tribunal, is too slow for the dynamic needs of recruiting in a competitive market.[49]

While the ADF's demography research concluded in 2006 that Generation Y tended to be less motivated by salary packages and more by the opportunities that jobs provide,[50] the continual adherence to this data in the face of market reality is arguably unhelpful. A more recent and targeted US study into shortages in the cyber security workforce found that rigid government

pay scales and complicated hiring practices make it difficult for the US Department of Defense to compete for the limited number of cyber operators.[51] Finding a more responsive pay structure for critical trades such as the cyber operator should therefore become a priority for workforce planners within the ADF.

So will geeks rule the military?

At this point, it may be useful to taper our vision of a future war against a fully-automated 'skynet' computer system,[52] with the realities of how significant remote operations will likely be in the foreseeable future. While it is clear that warfare is edging closer towards a transition that will require a review of how combatants are trained and recruited, it is unlikely that remote operators will become a significant portion of the ADF's personnel anytime soon. A range of ethical, functional and economic factors are all likely to constrain the rise of the warrior geek.

Ethically, the lack of any formal guidelines or laws which mandate the parameters or extent of human involvement in the decision-making processes of combat has allowed states to explore the increased use of robotics and artificial intelligence programs with impunity. While this supports Deptula's belief that remote wars protect against the vulnerability of human loss, the fear of war being waged without human involvement is a genuine concern for many. These fears are exacerbated by comments from remote operators referring to the game-like experience of RPA missions or their lack of emotional involvement in the conduct of cyber war.[53] So does the lack of an operator's proximity to war reduce it to an abstract activity?

In an effort to enhance the moral connectivity of remote operators, the US Army has developed 'The Human Dimension' training concept, which posits the central importance of the moral, physical and cognitive components of the soldier in order to provide a balance to the tactile tools of war.[54] In doing so, this theory highlights the pre-eminent need for a human element in war, not least to imbue ethical decision making in the face of increasingly remote methods of waging it, acknowledging the late British military historian Colonel Frederick Maude's comment that 'with every improvement in science, the result depends more and more on the character of the leader and his power of resisting the sensuous impressions of the battlefield'.[55]

Nevertheless, a study commissioned by the US Air Force suggests that remote operators are just as engaged as others involved in the fighting.[56] The report found that 20 per cent of RPA crews were suffering clinical distress, notwithstanding the missions being controlled from benign environments, which is comparable with the 28 per cent of soldiers returning from Iraq diagnosed with the same condition.[57] Findings such as these are systematically disproving the belief that remote wars are abstract events. More importantly, they are removing the ethical resistance to the rise of warrior geeks.

Beyond the ethical considerations, more practical experiences have blunted the adoption of a wholly remote method of warfighting. The widely-reported US war game 'Millennium Challenge 2002' demonstrated the shortfalls of over-reliance on networked systems.[58] In this activity, the networked 'blue force' was almost entirely destroyed within two days by an opposition using World War 2-era communication techniques to remain below detection thresholds. After the wargame was prematurely ended and reset, the 'red force' was ordered to employ systems that emit electronic signatures in order to assist blue force detection and targeting.[59]

The Millennium Challenge experience can provide several lessons regarding the reliance on network-enabled systems, including RPA and offensive cyber capabilities, as we look to their future employment. The first is that the success of unmanned platforms has largely been in operations where the airspace has not been contested, and where RPA have been able to loiter over target areas with relative impunity. The second is that remote and automated systems cannot win a war on their own, notwithstanding their growing utility. This reflects the truism that is relevant to all areas of military endeavour and is a driver behind the current focus on joint effects doctrine.[60]

Finally, the economic resistance to the rise of the warrior geek can be found in the tremendous cost of maintaining the current rate of technological advance. Moore's Law usefully reminds us that computing power is predicted to double every 18 months.[61] However, 'Augustine's Law' tempers that with the observation that the cost of technology increases exponentially.[62] Compounding that for the ADF are artificial pressures on defence capability expenditure, such as historically high rates of inflation, suggesting that RPA of the future—and projected acquisitions in general—will consume an ever-increasing portion of the defence budget.[63]

Conclusion

While the 2009 *Defence White Paper* discussed the intent for an increased unmanned and cyber capability, the scale of growth several years later remains quite modest. Seven large RPA and unspecified numbers of tactical aircraft and cyber operators do not represent a wholesale 'changing of the guard' in a force of over 57,000 uniformed personnel.[64] Nevertheless, the growth of a remote capability within the ADF will require progressive change, as the force adapts to the needs of a new information age.

Recognition of the unique operating environment for remote and cyber operators should predicate the need for an alternative approach to training. Remote wars are not physical contests, they are mental ones where no threat is posed to the operator. Consequently, traditional proximal skills, like marksmanship and first aid, which form the basis of current training approaches, will arguably become increasingly redundant. The remote operator needs different skills, such as advanced knowledge of sensors and the ability to manipulate systems in ways that exceed even the intentions of their designers. While the ADF is yet to integrate these skills into remote operator training, the courses being developed by the US Air Force offer models which could be adapted to local needs.

The growing demand for these skills is also likely to have a dramatic impact on the ADF's approach to recruiting. In order to access a greater portion of the limited cyber workforce, the ADF should reconsider its enlistment criteria to more closely reflect the needs of the job. This may entail reducing physical standards or reviewing the 'acceptable' criminal history of prospective remote operators. Consideration and further research should also be given to a more market-responsive pay structure for critical trades such as the cyber operator.

Finally, while it is accepted that the increased use of remote and cyber platforms will have a dramatic impact on the ADF's approach to training and recruiting methodologies, it is acknowledged that remote operators are unlikely to become a significant portion of the ADF's workforce anytime soon. And notwithstanding the seeming diminishing concerns regarding the ethical considerations for waging war through remote means, the practical ability to rely more fully on technological systems and the sheer cost involved in maintaining the current pace of change will continue to limit progress in the near term. What can be said, however, is that the rise of the 'warrior geek' is already marking a new era of how most future wars will be fought.

Lieutenant Colonel Tim Rutherford is a cavalry officer who graduated from RMC in 1999. He has held a range of command, planning and instructional appointments in Australia, Europe, the Middle East and Africa. He is a graduate of the Australian Command and Staff College and holds a Bachelor of Professional Studies (Peace Studies) and a Master of Military Studies. He is currently employed as the Staff Officer Grade 1 – Surveillance and Reconnaissance within Army Headquarters.

NOTES

1 P.W. Singer, *Wired for War*: *the robotics revolution and conflict in the 21st century*, Penguin: New York, 2009, p. 267.

2 C. von Clausewitz, *On War*, translated by M. Howard and P. Paret, Princeton University Press: Princeton, 1976, p. 53.

3 S. Gills, ‘Remaining Timely and Relevant: two key challenges for army’s intelligence capability post-Afghanistan’, *Australian Army Journal*, Vol. IX, No. 2, 2012, pp. 59-82.

4 G. Conti and D. Raymond, 'Leadership of Cyber Warrior: enduring principals and new directions', *Small Wars Journal*, 11 July 2011.

5 US Department of Defense, ‘DOD Announces First US Cyber Command and First US Cyber Command Commander’, media release, 21 May 2010, available at <http://www.defense.gov/releases/release.aspx?releaseid=13551> accessed 8 September 2014.

6 C. Hanna,'Cyber Operations and the 2009 Defence White Paper: positioning the ADO to be effective, transparent and lawful', *Security Challenges*, Vol. 5, No. 4, 2009, pp. 103-17.

7 For a comprehensive list of alternative terms, see: W. Howse, ‘Knowledge, Skills, Abilities, and Other Characteristics for RPA Pilots Operators’, Strategic Research and Assessment Branch, Air Force Personnel Centre: Randolph Air Force Base, Texas, 2011, p. 1.

8 K.W. Bucklew, ‘Non-traditional ISR: a challenge to fixed wing tactical aircraft’, Marine Corps University, Marine Corps Development Command: Quantico, 2009, p. 3.

9 Department of Defence, *White Paper - Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia: Canberra, 2009.

10 Department of Defence, *White Paper - Defending Australia in the Asia Pacific Century*, p. 80.

11 Department of Defence, *Defence Capability Plan*, Commonwealth of Australia: Canberra, 2012, p. 63.

12 M. Howard, 'Air Force Safety Centre - Aircraft Mishap Comparison', Presentation to the CNS-ATM Conference, 13 June 2011, available at <http://www.afceaboston.com/documents/events/cnsatm2011/Briefs/03-Wednesday/Wednesday-PM%20Track-2/02-LtCol%20Howard-GBSAA%20Safety%20Case-%20Wednesday%20Track2.pdf> accessed 8 September 2014.

13 Howse, ‘Knowledge, Skills, Abilities, and Other Characteristics for RPA Pilots Operator’, p. 40.

14 Peter La Franchi, quoted in M. Corcoran, ‘The Kill Chain: Australia’s drone war’, Foreign Correspondent, ABC website, 27 June 2012, available at <http://www.abc.net.au/news/2012-06-08/australias-drone-war-in-afghanistan/4058058 accessed 8 September 2014>. An additional review of the ADF’s planned expenditure on unmanned platforms from 2007-12 offered figures between $370.9 million and $740 million. For more, see M. Thompson, 'The Cost of Defence: ASPI Defence budget brief 2007-08', Australian Strategic Policy Institute (ASPI): Canberra, 2007; and M. Thompson, 'The Cost of Defence: ASPI Defence budget brief 2014-15', ASPI: Canberra, 2014.

15 L. Baldor, 'The Next Top Guns? Air Force faces shortage of drone pilots', *Associated Press*, 8 September 2012, p. 3

16 Department of Defence, *Defence White Paper 2013*, Commonwealth of Australia: Canberra, 2013, p. 78

17 This includes the Australian Federal Police, national intelligence services and the Attorney General’s Department, which is Australia’s lead agency for e-security. For more, see Department of Defence, ‘Cyber Security Operations Centre Officially Opened’, media release, 15 January 2010; Department of Defence, *Defence Capability Plan*, pp. 113-23; and Department of Defence, ‘Commissioning of New Supercomputer at the Defence Signals Directorate’, media release, 18 March 2010.

18 K. Alexander, ‘Statement to the Senate Committee on Armed Services’, 20 March 2012, available at <http://www.armed-services.senate.gov/statemnt/2012/03%20March/Alexander%2003-27-12.pdf> accessed 27 May 2014.

[19] J. Stern, ‘Pentagon Cyber Command: higher status recommended’, *ABC World News*, 2 May 2012, available at <http://abcnews.go.com/Technology/pentagon-cyber-command-unit-recommended-elevated-combatant-status/story?id=16262052> accessed 25 May 2014.

[20] A review of recruit course content for the Australian Army, Navy and Air Force can be found respectively at: <http://www.defencejobs.gov.au/army/training/soldier.aspx, http://www.navy.gov.au/join-navy/recruit-school/course-content, http://www.airforce.gov.au/docs/1RTU%20Joining%20Instruction%202012.pdf>

[21] G. Conti and J. Surdu, 'Army, Navy, Air Force, and Cyber - Is it Time for a Cyberwarfare Branch of Military', *Information Assurance*, Vol. 12, No. 1, 2009, p. 15.

[22] C.M. Hardison, M.G. Mattock and M.C. Lytell, 'Incentive Pay for Remotely Piloted Aircraft Career Fields', RAND Corporation: Santa Monica, 2012, p. 34.

[23] Highlighting the growing interest and complexity in RPA, tertiary institutions such as Indiana State University now offer minor programs in unmanned systems. For more, see Indiana State University, ‘Unmanned Systems’, College of Technology website, available at <http://technology.indstate.edu/uas/index.htm> accessed 4 May 2014. For a more detailed review of the undergraduate program mentioned in the text, see Hardison *et al*, 'Incentive Pay for Remotely Piloted Aircraft Career Fields', pp. 9-10; and J.A. Tirpak, 'Putting the Pilot in the RPAs', *Air Force Magazine*, July 2010, p. 63.

[24] J. Andress, S. Winterfeld and R. Rogers, *Cyber Warfare: techniques, tactics and tools for security practitioners*, Elsevier: Boston, 2011, pp. 68-9.

[25] K. Evans and F. Reeder, 'A Human Capital Crisis in Cybersecurity', Centre for Strategic and International Studies: Washington, 2010, p. vi.

[26] M.G. Beach, 'Managing Cyber Operator Training Curriculum', Air Force Institute of Technology: Wright-Patterson Air Force Base, Ohio, 2010, pp. 26-8.

[27] Beach, 'Managing Cyber Operator Training Curriculum', pp. 26-8.

[28] Conti and Surdu, 'Army, Navy, Air Force, and Cyber - Is it Time for a Cyberwarfare Branch of Military’, p. 17.

[29] Conti and Surdu, 'Army, Navy, Air Force, and Cyber - Is it Time for a Cyberwarfare Branch of Military', pp. 16-7.

[30] Hanna, 'Cyber Operations and the 2009 Defence White Paper’, p. 113.

[31] Hanna, 'Cyber Operations and the 2009 Defence White Paper’, p. 113.

[32] D. Deptula, ‘US Military Use of Drones’, *CNN* transcripts, 29 November 2009, available at <http://transcripts.cnn.com/TRANSCRIPTS/0911/29/ampr.01.html> accessed 5 May 2014.

[33] Summary of the ADF’s recruitment process, cited in Australian Human Rights Commission, *Review into the Treatment of Women in the Australian Defence Force, Phase 2 Report*, Australian Human Rights Commission: Sydney, 2012, p. 109.

[34] Alexander, ‘Statement to the Senate Committee on Armed Services’, p. 14.

[35] Jim Gosler, a visiting scientist at the US National Security Agency and founding director of the Clandestine Information Technology Office within the CIA, stated there were approximately 1,000 specialists in the US with the skills to operate effectively in cyberspace; however, between 10,000 and 30,000 are needed. For more, see J. Gosler, ‘Cyberwarrior Shortage Threatens US Security’, *NPR Morning Edition*, 19 July 2010, available at <http://www.npr.mobi/templates/transcript/transcript.php?storyId=128574055> accessed 22 May 2014.

[36] L. Ponemon, ‘Global Cost of Data Breach’, Security Research Studies and White Papers, Ponemon Institute: Michigan, 2011, p. 2.

[37] Noetic Solutions, 'Review of the Australian Defence Force Retention and Recruitment Strategy', Report for the Department of Defence, Noetic Solutions: Canberra, 2010, p. 25, available at <http://www.defence.gov.au/foi/docs/disclosures/234_110520_neotic_evaluation_report_may_2010.pdf> accessed 8 September 2014.

[38] Conti and Raymond, 'Leadership of Cyber Warrior’, p. 3.

[39] Conti and Raymond, 'Leadership of Cyber Warrior’, p. 4.

[40] Howse, 'Knowledge, Skills, Abilities, and Other Characteristics for RPA Pilots Operator'.

[41] The RAAF currently manages the ADF's large RPA and cyber operations units. A review of its recruit course highlights the central focus on physical fitness throughout the recruitment and *ab initio* training phases. For more, see Hanna, 'Cyber Operations and the 2009 Defence White Paper', pp. 103-17; and W.F.H. Merkx, 'Recruit Joining Instructions', 1 Recruit Training Unit, RAAF: Wagga Wagga, 2012.

[42] O. Garcia and S. Burgos, 'Relationship between Physical Prowess and Cognitive Function', *Spanish Journal of Psychology*, Vol. 15, No. 1, 2012, p. 33.

[43] Garcia and Burgos, 'Relationship between Physical Prowess and Cognitive Function', p. 33.

[44] Andress, Winterfeld and Rogers, *Cyber Warfare*, p. 67.

[45] K. Thomas and S. Bell, 'Competing for the Best and Brightest: recruitment and retention in the Australian Defence Force', *Security Challenges*, Vol. 3, No. 1, 2007, p. 111.

[46] R. Carroll, 'US Urged to Recruit Master Hackers to Wage Cyber War on America's Foes', *The Guardian*, 10 July 2012, available at <http://www.guardian.co.uk/technology/2012/jul/10/us-master-hackers-al-qaida> accessed 24 May 2014.

[47] Originally defined by McAfee internet security, the hats classification consisted of 'white' and 'black', which essentially translated to good or bad intention. This was progressed by Darren Thomas, who included 'grey' for those hackers in between. For a more detailed discussion, see McAfee, 'Who are hackers: where do they come from and why are they called hackers?', *E-security News*, 2002, available at <http://dispatch.mcafee.com/esecuritynews/jan2002/firewallforum.asp> accessed 19 May 2014; and D. Thomas, 'Art of War, Part3', infosecnews blog, 6 August 2003, available at <http://www.infosecnews.com/opinion/2003/08/06_01.htm> accessed 19 May 2014.

[48] C. Fitch, *Crime and Punishment: the psychology of hacking in the new millennium*, SANS Institute: Bethesda, 2004, p. 5.

[49] Department of Defence, 'Defence Force Remuneration Tribunal', Defence Personnel Executive website, available at <http://www.defence.gov.au/dpe/pac/DFRT.htm> accessed 1 May 2014.

[50] J. Hearps, A. Cohn, J. Temple and P. McDonald, 'Defence Personnel Environment Scan 2025', Directorate of Strategic Personnel Planning and Research, Department of Defence: Canberra, 2006, p. 30.

[51] S. Hawald and S. Bittinger, 'How Government/DoD CIOs Can Deal with the Cybersecurity Workforce Shortage' Gartner Industry Research: Washington, 2012, p. 1, available at <https://www.gartner.com/doc/2115517/governmentdod-cios-deal-cybersecurity-workforce> accessed 9 September 2014.

[52] 'Skynet' refers to the automated computing system in the movie series 'The Terminator', which becomes 'self-aware' and instigates a war with its human controllers that results in a nuclear holocaust.

[53] For an excellent discussion on the ethical and legal considerations for remote operations, see Singer, *Wired for War*, pp. 330-4; S.R. McGrath, 'Strategic Misstep: "immoral" robotic warfare, inviting combat to suburban America', US Army War College: Carlisle, 2010, pp. 32-3; and B. Baker, 'Locked and Loaded – the Ethics of Armed Drones', airforce-technology.com website, 2011, available at <http://www.airforce-technology.com/features/feature130337> accessed 29 May 2014.

[54] US Department of the Army, 'The US Army Concept for the Human Dimension in Full Spectrum Operations, 2015-2024', Department of Defense: Washington, 2008, pp. 3-8.

[55] F.N. Maude, 'Introduction', in C. von Clausewitz, *On War*, translated by J.J. Graham and F.N. Maude, Wilder Publications: Radford, 1909, p. iii.

[56] W. Chappelle, K. McDonald, B. Thompson and J. Swearengen, 'Prevalence of High Emotional Distress and Symptoms of Post-Traumatic Stress Disorder in US Air Force Active Duty Remotely Piloted Aircraft Operators', US Air Force Research Laboratory: Wright Patterson Air Force Base, 2012, p. 1, available at <www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA577055> *accessed 13 September 2014.*

[57] Quoted in P. Stewart, 'Overstretched US Drone Pilots Face Stress Risk', *Reuters*, 19 December 2011 available at <http://www.reuters.com/article/2011/12/19/us-drone-pilots-stress-idUSTRE7BI24N20111219> accessed 15 September 14. Several studies are currently being undertaken to refine the understanding of stress on remote operators. For more, see M. Christen, M. Villano, D. Narvaez and C. Crowell, 'Measuring the Moral Impact of Operating "Drones" on Pilots in

Combat, Disaster Management and Surveillance', Twenty Second European Conference on Information Systems, Tel Aviv, 2014, available at <http://ecis2014.eu/E-poster/files/0829-file1.pdf> accessed 15 September 2014.

58 D. Chisholm, 'Organisational Change in Uncertain Times: the US Military and Millennium Challenge 2002', Address to Naval War College, 23 September 2002, Rhode Island, available at <http://web.mit.edu/ssp/seminars/wed_archives02fall/chisholm.htm> accessed 25 May 2014; and D. von Lubitz, 'What We Should Have Learned From MC02', Defense and the National Interest, Project on Government Oversight: Washington, 2008.

59 Chisholm, 'Organisational Change in Uncertain Times' and von Lubitz, 'What We Should Have Learned from MC02'.

60 Department of Defence, *Australian Defence Doctrinal Publication D.3: Joint Operations for the 21st Century*, Department of Defence: Canberra, 2007.

61 While Gordon Moore's original observation was made with specific reference to the complexity of minimum cost semi-conductor components, it was broadened over subsequent decades to include microprocessor power. It now underpins all predictions on the future capability of computing technology. For his original article, see G. Moore, 'Cramming More Components onto Integrated Circuits', *Electronics*, Vol. 38, No. 8, 1965. For a contemporary discussion on the evolution and merit of Moore's Law, see I. Toumi, 'The Lives and Death of Moore's Law', *First Monday*, Vol. 7, No. 11, 2002; or G.C. Chow, 'Technological Change and the Demand for Computers', *American Economic Review*, Vol. 57, No. 5, 1967, pp. 1117-30.

62 Defence industry commentator and former chairman of Lockheed Martin, Norman Augustine's so-called Augustine's Law states that 'Defense budgets grow linearly but the cost of military aircraft grows exponentially'. For more, see N.R. Augustine, 'Augustine's Laws', *American Institute of Aeronautics and Astronautics*, 1997, p. 107.

63 A. Davies, 'The Capability Process and Defence Projects', presentation on Planning Capability, Module 10, Session 5, at Australian Command and Staff College, Canberra, 25 July 2012.

64 Noetic Solutions, 'Review of the Australian Defence Force Retention and Recruitment Strategy', p. 5.

Improving the Australia-India Relationship – A Naval Focus [1]

Captain Katherine Richards, CSC, RAN

> It is time that both countries 'move well beyond the three Cs: curry, cricket and the Commonwealth'.
>
> Rajaram Panda and Pranamita Baruah, 2010 [2]

Introduction

Australia and India share 'the values of entrepreneurial capitalism and political pluralism'.[3] Yet beyond their democratic traditions, a shared love of cricket and Commonwealth membership, the strategic relationship between the two nations has been described as a 'relationship that's always about to "take-off" but never does'.[4]

Yet, others have argued that 'the threefold logic of geography, economics and regional security is pushing India and Australia closer'.[5] Moreover, historic differences 'are being steadily erased by a desire for greater cooperation on common goals and closer trade links'.[6] And there seems to be broad agreement that Australian and Indian strategic interests are converging, with this convergence most keenly felt in the maritime domain.[7]

This article asserts that, as part of that convergence, the bilateral security relationship between India and Australia could be improved, at least in part, through greater knowledge-sharing between the RAN and the Indian Navy (IN). In the short term, this type of exchange could lead to deeper people-to-people linkages between the two while, in the longer term, these linkages could lead to greater cooperation in the field of maritime security.

The article begins with a brief overview of the Australia-India strategic relationship, including its policy settings and challenges. It then outlines a number of initiatives, for senior officers, mid-ranking officers and junior officers, which could provide greater depth to the RAN/IN relationship as a contribution towards improved Australia-India relations.

An overview of the strategic relationship

The Australia-India strategic relationship is a relatively recent innovation when compared to the bilateral trade links, which have their origins in the early days of the Botany Bay settlement.[8] In August 2001, Australia and India held the first Australia-India Strategic Dialogue in New Delhi.[9] Seven years later, in 2008, the Chiefs of the respective Defence Forces agreed to meet annually.[10] In 2009, Australia's Defence White Paper described India as an 'important partner'.[11]

Later that year, Australia and India also signed the 'India-Australia Joint Declaration on Security Cooperation', which was seen as a 'notable step in the process of developing a closer security relationship with India'.[12] Australia's most recent Defence White Paper (2013) states that 'our Navy to Navy relationship continues to grow—a natural progression given our shared maritime security interests as Indian Ocean littoral states'.[13]

Today, the Australia-India strategic relationship reveals a spectrum of cooperation that includes high-level visits, ongoing exchanges, dialogues and ship visits.[14] However, some contend that the relationship has actually 'achieved remarkably little in matters related to hard conventional security' and that 'operational coordination between the two militaries remains weak'.[15] Furthermore, despite the 'many opportunities open for collaboration in security, practical security cooperation between India and Australia has been slow to develop' and, in practice, 'Australia and India are still a long way from having a close working security relationship'.[16]

Some of the constraints and limitations

The lack of depth in Australia-India security cooperation is in many ways a reflection of the considerable challenges in developing the strategic relationship. In the first instance, economic forces and not security dynamics have traditionally dominated the bilateral relationship. This means that 'Canberra does not enjoy a high degree of priority in New Delhi'; rather, 'Australia appears to have little to offer beyond natural resources'.[17]

Second, the strategic cultures and traditions of New Delhi and Canberra are markedly different. India's strategic culture is centred on independence and a 'cherished goal' of strategic autonomy.[18] In contrast, notions of collaboration and an implied assumption of working in coalitions dominate Australia's strategic culture.[19] The impact of these cultures is that India remains 'highly suspicious of foreign engagements', and exercises 'extreme caution' in agreeing to any form of security cooperation with other countries.[20]

Furthermore, other barriers to cooperation include the Indian perspective that Australia is not generally seen as an 'independent' strategic actor due to its close relationship with the US,[21] and a reluctance by some in India 'to treat Australia on an equal basis'.[22] Also, divergent views on China's intentions in the Indian Ocean, and Australia's cooperation with Pakistan further detract from stronger cooperation.[23] When all these factors are combined with the limitations of a small bureaucracy hamstrung by 'bureaucratic inertia',[24] the result is that 'Indian officers and civil servants who are actually in charge of the operational aspects of the relationship are still uncomfortable cooperating with their counterparts from other countries'.[25]

At the strategic level, the net effect of these challenges is that 'New Delhi is yet to be convinced that engagement with a middle power such as Australia is a high priority relative to other commitments'.[26] Consequently, cooperation is largely restricted to 'soft security and dialogues'.[27] Moreover, while good personal relationships between respective Service Chiefs exist, there remains a 'thinness of interaction at other levels'.[28] As such, dialogues have been characterised by some observers as 'frequently more form over substance'.[29]

Given the numerous challenges to developing the relationship, Michael Wesley counsels that 'engaging India strategically... will take many years'.[30] However, addressing the 'thinness' of the people-to-people relationships below the Service Chief level is one aspect of the relationship that can be addressed now. Given that Australia and India have shared maritime interests and 'the two most advanced navies of the Indian Ocean rim countries',[31] deepening the linkages between the RAN and the IN is a logical starting point for any improvements aimed at bringing depth to the bilateral strategic relationship.

Deepening the Navy-to-Navy linkages

David Brewster contends that 'the development of people-to-people networks is an extremely important factor in developing the India-Australia security relationship'.[32] He further notes that the 'development of personal relationships and experiences of policy makers, military officers and civilians in the security community can provide the crucial long-term and sorely-needed glue in the bilateral relationship'.[33]

Australia and India have an established, though small, people-to-people military officer network. In recent years, participation in the Indian Ocean Naval Symposium (IONS) has expanded this network and also led to stronger and broader naval relationships throughout the Indian Ocean region. Student exchanges at each nation's respective junior and senior staff courses have also contributed to the people-to-people military officer network.[34] However, notwithstanding the professional development value of these courses, they do not specifically target common naval interests and hence only indirectly shape the Navy-to-Navy relationship.

Accordingly, this article proposes that the RAN/IN relationship could be further enhanced by knowledge-sharing activities which directly address the challenges of modernisation and

capability development for senior and mid-rank officers, together with a cultural familiarisation program for junior officers.

Shared interests in fleet modernisation and capability development

Both the RAN and IN are grappling with the concurrent challenges of major fleet modernisation programs, while simultaneously sustaining legacy systems. The centerpiece of the RAN's modernisation program is the acquisition of new surface combatants. These include two major amphibious ships and three new air warfare destroyers. These programs are supported by the acquisition of new squadrons of rotary wing aircraft (MRH90 Taipan and MH60R Seahawk) and planning for the replacement submarine for the Collins class.

Similarly, the IN's modernisation program includes virtually all classes of combatants, with a forward order book of some 40 ships and six submarines.[35] Furthermore, the bulk of these combatants are indigenous builds, including the aircraft carrier INS *Vikrant* and the nuclear-powered submarine INS *Arihant*.

However, both nations have experienced significant problems with recent past acquisitions, current projects and sustainment of their fleets-in-being. For the RAN, the Collins class submarine and the ill-fated Sea Sprite helicopter projects are textbook examples of what can go wrong with major maritime acquisitions.[36] The major schedule delay with the Air Warfare Destroyer Project also demonstrates the complexity of Australian indigenous build programs. Moreover, the RAN has also been roundly criticised in recent years for its failures in operational availability stemming from a chronic under-investment in engineering and maintenance services for its support ships.[37]

For the IN, its indigenous defence production is reportedly 'marred by serious technical and organisational problems, leading to significant delays in the development of key defence technologies and platforms'.[38] Examples include major delays in the introduction into service of the carrier, the Kolkata class destroyers and the Scorpene class submarines.[39] Additionally, beyond the numerous problematic acquisition programs, the IN also has a 'poor accident record' with several deaths reported during build, maintenance and operational activities in recent years.[40]

For the Navy-to-Navy relationship, however, the challenges of modernisation represent an opportunity for the RAN and IN to deepen their engagement through knowledge-sharing. This could be achieved through an annual 'Acquisition and Sustainment' dialogue between senior naval officers (at the O6-O7 level) responsible for the delivery of key programs. The dialogue could run in parallel and complement the annual strategic level engagement between the RAN and IN Chiefs of Navy.

In establishing the dialogue, the RAN may have to accept that the IN may not have the institutional capability to act in a reciprocal manner[41] or may be non-committal or sensitive to the nature of some of its modernisation problems, particularly in relation to safety concerns. Over time, however, provided the RAN remains patient, the dialogue has the potential to bring real substance to the people-to-people relationships.[42]

Moreover, as trust and confidence grows, the dialogue could be readily expanded to address other areas of possible interest, such as commercial risk assessments, engineering and maintenance innovations, and the RAN's concept of seaworthiness. All of these areas have the potential to demonstrate to India the inherent value of engaging with the RAN specifically, and more broadly with Australia.

The shared challenges in acquisition and sustainment also open the possibilities for Australia to invite India to send a naval representative to the Capability and Technology Management Course (CTMC). It is a 12 months Masters program (at the O5-O4 level), run by the University of New South Wales at the Australian Defence Force Academy in Canberra. The aim of the course is to provide graduates with the requisite skills in military science and technology, capability management and capability staff skills in order to enhance Defence capability development,

acquisition and sustainment.[43] The course includes a dedicated 'Maritime Technologies' subject, which examines case studies of both Australian and international maritime projects.

For an IN student, the course would provide a deep insight into the theory and practice of project management and the ADF's capability development processes. More broadly, the offer of a student place on CTMC aligns with current government policy whereby the delivery of education services is seen as 'in our national interest and a core part of our 'soft diplomacy' in the region.[44] In terms of practical execution, the CTMC has capacity for 44 personnel and typically works on an overseas course member allocation of approximately ten per cent.[45] Discussions with the Director of CTMC revealed that he would welcome greater regional participation from the Indo-Pacific and, given the scale of the IN's modernisation program, an IN student would be highly valued.

Building understanding: a bottom-up approach

Beyond initiatives to address the challenges of modernisation, developing a deeper cultural understanding between the RAN and IN is a further area that warrants attention. Michael Wesley contends 'there is a remarkable lack of understanding in each society about the contemporary realities in the other, and a depressing reliance on stereotypes and dated information'.[46] Moreover, Sally Percival Wood opines that 'deepening ties between Australia and India will depend upon the quality of, and commitment to, our mutual understanding'.[47]

Against this backdrop, one option open to the RAN to address these issues could be an extension of its 'observer-at-sea' program to target junior IN officers during routine Southeast Asian and Northeast Asian deployments. The provision of sea-riding opportunities on transits between Indo-Pacific ports could be utilised for RAN cultural familiarisation for IN junior officers. Such a program may also help to overcome the tyranny of distance for IN officers in travelling to Australia and the general reluctance of the IN to send junior officers to Australia for lengthy training at the Australian Defence Force Academy.[48]

Costs associated with the program are likely to be minimal and limited to airfares to and from India to ports such as Singapore, Jakarta, Bangkok and Manila. In the longer term, the program could also help to develop friendships and camaraderie between a cohort of junior RAN and IN officers, out of which an understanding of culture, political processes, values, interests and, ultimately, maritime security could grow.

Conclusion

It is just 14 years since Australia and India established their strategic relationship. High-level dialogues, ship visits and exchanges have played a role in developing this relationship, however, it still lacks depth. 'Hard' security cooperation has not been achieved, largely due to the hurdles of bureaucratic inertia, divergent strategic cultures and Canberra's middle-power status.

Given these constraints, a focus on shared maritime interests and, in particular, bringing the RAN and IN closer together through stronger people-to-people relationships is likely to be the key to creating a more comprehensive strategic relationship. This could be achieved by leveraging off the lessons learned from parallel modernisation programs and by undertaking cultural familiarisation transits in the Indo-Pacific.

The success of these initiatives, and any others, will be predicated on Australia taking a long-term view of the relationship and then proceeding with patience. For ultimately, to improve the bilateral relationship, it is Australia that will need to demonstrate that it is more than just another middle power eager to gain from India's rise.

Captain Katherine Richards is a Marine Engineer Officer who has served in the RAN for 25 years. She spent much of her early career at sea in HMAS Canberra and HMAS Newcastle, and working in waterfront engineering roles. She was part of the commissioning crew of the Leeuwin-class hydrographic ships and served as the Marine Engineer Officer in HMAS Melbourne. During her time at sea, Captain Richards participated in operations in the Southern Ocean (Operation STANHOPE), the Solomon Islands (Operation TREK) and the Persian Gulf (Operation SLIPPER).

Her more recent appointments have included Staff Officer to VCDF, Directing Staff at the Australian Command and Staff College, and Director of the LHD Systems Program Office in the Defence Materiel Organisation, as well as Command of HMAS Cerberus. She has a Bachelor of Engineering with 1st Class Honours from the University of NSW, a Masters of Science in Marine Engineering from University College London and a Masters of Management in Defence Studies from the University of Canberra. She is currently attending the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College.

NOTES

[1] This is an edited version of a paper developed by the author while attending the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College in 2014.

[2] Rajaram Panda and Pranamita Baruah, 'India-Australia Strategic Partnership: a case for holistic approach', *India Quarterly*, Vol. 66, No. 2, 2010, p. 217. Of course, the reference to the 3Cs pre-dates its use by Panda and Baruah: see, for example, the assertion by Richard Woolcott, 'Beyond Cricket and Curry Accord', *Sydney Morning Herald*, 2 April 2010, in which he asserts the relationship has already 'moved well beyond the three Cs', available at <http://www.smh.com.au/federal-politics/society-and-culture/beyond-curry-and-cricket-accord-20100401-rhxx.html> accessed 13 October 2014. The 3Cs are also sometimes used in relation to the Australia-Pakistan relationship.

[3] C. Raja Mohan, 'India and Australia: maritime partners in the Indo-Pacific', *The Asia Link Essays*, Vol. 3, No. 6, November 2011, p. 4.

[4] Greg Sheridan quoted in Sam Bateman and Anthony Bergin, 'Our Western Front, Australia and the Indian Ocean', Australian Strategic Policy Institute: Canberra, March 2010, p. 34.

[5] Raja Mohan and Rory Medcalf, 'Two nations take lead in securing Indo-Pacific century', Commentary Piece, 24 June 2013, Lowy Institute website, available at <http://www.lowyinstitute.org/publications/two-nations-take-lead-securing-indo-pacific-century> accessed 23 July 2014.

[6] The Diplomat, 'Australia-India Relations', The Diplomat website, 2 February 2009, available at <http://thediplomat.com/2009/02/australia-india-relations/> accessed 24 July 2014.

[7] Frederic Grare, *The India-Australia Strategic Relationship, Defining Realistic Expectations*, Carnegie Endowment for National Peace: Washington DC, 2014, p. 24.

[8] Peter Varghese, 'Our Journey with India', Address by the Secretary Department of Foreign Affairs and Trade, Australia-India Institute Oration, 16 May 2013.

[9] Panda and Baruah, 'India-Australia Strategic Partnership', p. 208.

[10] Panda and Baruah, 'India-Australia Strategic Partnership', p. 209.

[11] This was based on 'shared democratic values, maritime interests, a commitment to combating regional and global terrorism and the maintenance of a rules based global security order': Australian Government, *Defending Australia in the Asia-Pacific Century Force 2030 (Defence White Paper)*, Department of Defence: Canberra, 2009, p. 96.

[12] David Brewster, 'The Australia-India Security Declaration: the quadrilateral redux?', *Security Challenges*, Vol. 6, No.1, Autumn 2010, p. 1.

13 Australian Government, *Defence White Paper*, Department of Defence: Canberra, 2013, p. 65.

14 The dialogues cover key areas such as information sharing, counter terrorism and peace-keeping: Australian Government, *Defence White Paper 2009*, Department of Defence: Canberra, p. 96.

15 Grare, *The India-Australia Strategic Relationship,* p. 7.

16 Dennis Rumley (ed.), 'The Indian Ocean Region: security, stability and sustainability in the 21st century', Australia India Institute, University of Melbourne: Melbourne, March 2013, p. 92, available at <http://apo.org.au/research/indian-ocean-region-security-stability-and-sustainability-21st-century> accessed 13 October 2014.

17 Grare, *The India-Australia Strategic Relationship*, p. 24.

18 David Brewster, 'The India-Australia Security Engagement: opportunities and challenges', Gateway House Research Paper No. 9, October 2013, p. 38.

19 Brewster, 'The India-Australia Security Engagement'*,* p. 38.

20 Brewster, 'The India-Australia Security Engagement', p. 39.

21 Brewster, 'The Australia-India Security Declaration', p. 7.

22 Bateman and Bergin, 'Our Western Front, Australia and the Indian Ocean'*,* p. 35.

23 Brewster, 'The Australia-India Security Declaration', p. 41.

24 Brewster, 'The Australia-India Security Declaration', p. 44.

25 Grare, *The India-Australia Strategic Relationship*, p. 24.

26 Rumley, 'The Indian Ocean Region', p. 92.

27 Grare, *The India-Australia Strategic Relationship*, p. 6.

28 Brewster, 'The India-Australia Security Engagement', p. 35.

29 Brewster, 'The India-Australia Security Engagement', p. 35.

30 Michael Wesley, 'The Rise of India', *Policy*, Vol. 27, No. 3, Spring 2011, p. 45.

31 Stephen Smith, 'Australia and India: building the strategic partnership', Address by the Minister for Defence of Australia, Asia Society, Mumbai, 9 December 2011.

32 Brewster, 'The India-Australia Security Engagement', p. 54.

33 Brewster, 'The India-Australia Security Engagement', p. 54.

34 Typically just two mid-rank officers (O-5) and two senior-rank officers (O-6) participate in these exchanges per annum.

35 Vishnu Som, 'On INS Kolkata PM is only partially correct', available at <http://www.ndtv.com/article/opinion/on-ins-kolkata-pm-is-only-partially-correct-576698> accessed 20 August 2014.

36 For full details on the problematic Collins class build program refer to Peter Yule and Derek Woolner, *The Collins Class Submarine Story, Steel, Spies and Spin*, Cambridge University Press: Port Melbourne, 2008. For a summary of the major problems of the Super Sea Sprite Program refer to the Australian National Audit Office report, available at <http://www.anao.gov.au/Publications/Audit-Reports/2008-2009/The-Super-Seasprite> accessed 20 August 2014.

37 For full details refer to Paul J. Rizzo, *Plan to Reform Support Ship Repair and Maintenance Practices*, Commonwealth of Australia: Canberra, July 2011.

38 Harsh V. Pant, 'Challenges to India's Indigenous Naval Build Up', 22 September 2013, *Japan Times* website, available at <http://www.japantimes.co.jp/opinion/2013/09/22/commentary/world-commentary/challenges-to-indias-indigenous-naval-buildup/> accessed 24 August 2014.

39 N. C. Bipindram, 'Submarine project delayed due to government apathy', 8 April 2013, *New Indian Express* website, available at <http://www.newindianexpress.com/nation/article1535565.ece> accessed 17 August 2014.

40 Pant, 'Challenges to India's Indigenous Naval Build Up'.

41 Brewster, 'The India-Australia Security Engagement', p. 46.

42 Michael Wesley contends that ‘the challenge of building a closer Indo-Australian relationship will lie in the encounter between an impatient Australia and a non-committal India’: see Michael Wesley, ‘The Elephant in the Room’, *The Monthly*, February 2012, p. 36.

43 P.B. Spencer, ‘CTMC Course Overview’, Chief Instructor CTMC (unpublished paper), 22 August 2014.

44 Julie Bishop, ‘Charting the future of Australia-India relations’, *Australian Polity*, Vol. 2, No. 3, available at <http://australianpolity.com/category/australian-polity/page/5> accessed 1 August 2014.

45 The 2014 CTMC has regional representatives from Indonesia, Thailand, New Zealand and Malaysia.

46 Wesley, ‘The Rise of India’, p. 45.

47 Sally Percival Wood, ‘“So where the bloody hell are we?”: the search for substance in Australia-India relations’, The Fearless Nadia Occasional Papers on India-Australia Relations, Australia India Institute, Vol. 1, Winter 2011, p. 1.

48 Brewster, ‘The India-Australia Security Engagement’, p. 46.

The Contribution of Submarines to Canada's Freedom of Action on the World Stage [1]

Professor Paul T. Mitchell, Canadian Forces College

Introduction

Recent generator problems experienced by HMCS *Windsor* have once again put Canada's troubled submarine program back into the public spotlight.[2] Many Canadians are outraged by the continuing problems our submarines experience and naturally question the rationales under which they have been acquired. It almost seems that the image problem the submarine service endures is the biggest threat Canadian submariners confront. The selective nature of this attention must be particularly frustrating, as other accidents and incidents within the Royal Canadian Navy (RCN) fail to attract similar levels of public concern.[3]

In this environment, the more difficult job should be convincing Canadians of the need to invest in a submarine capability for the navy. The real irony is that this debate on Canadian naval capability is so narrowly focused on a single weapon system. The real argument that needs to be made forcefully is that Canada's navy requires a combined arms team that includes a variety of platform types in the air and at sea—such a formation deeply at risk with the obsolescence of our air defence destroyers and the erosion of at-sea logistic support.

Nevertheless, the task at hand today is to argue for the role of submarines in that combined arms team. As such, this article will dispute the arguments advanced concurrently by Michael Byers,[4] and then establish that the strategic capabilities afforded by submarines make them not only a critical part of that maritime combined arms team but also among the most cost effective platforms for protecting Canadian interests in a rapidly-changing international environment.

Unfit weapon systems?

Canada's existing submarines have developed a reputation as 'lemons' among the public, largely because of a series of unfortunate incidents. This has been reinforced by the delay in getting the boats operational, an impact that speaks more to stresses stemming from a tight budget for operations and maintenance during a period of wartime operations.[5] The RCN also took some risk in acquiring an 'orphan system', which complicated the establishment of a logistics system to support on-going operations.[6] Again, none of this has anything to do with deficiencies in the construction or design of the boats, and speaks only to the shoestring budget under which the RCN acquired the submarines in the 2000s.

Two features explain some of the difficulties that Canadian submarines have experienced in their long road to operational status. First is the level of their technical sophistication and the high demand this places on the professionalism of their crew. The Victoria-class submarines are among the quietest submarine systems in the world. They share key technological systems with Britain's Trafalgar-class nuclear submarines, highly sophisticated and classified features that must be expertly used if they are to be effective.

Second, the very environment in which submarines operate also places a premium on professional excellence. Submarines share more in common with space programs than they do with other naval programs. The unforgiving nature of working at depth is akin to working in the vacuum of space: errors of tactical judgment and operational protocols can be instantly lethal. While safety is always a concern for professional mariners, it assumes an existential priority for submariners. It is for both these reasons that the course for command qualification in submarines is traditionally called 'Perisher'.[7]

These two aspects mean that maintaining an effective operational capability implies significant investments in infrastructure and training regimes to generate effective operational practice (and experience). The length of time the Canadian Government took in the decision to acquire the submarines meant that both of these had significantly atrophied in the intervening period. This had to be expensively rebuilt in the last decade, and at the same time that significant naval operations were being conducted in support of the 'War on Terror'. This, rather than supposed deficiencies in the design of Canada's submarines, explains their long road to operational capability.

All we need is a war ... with China

Byers devotes an extended consideration to the RCN strategic concept called *Horizon 2050*, which argues that 'we should anticipate the possible re-emergence of inter-state maritime armed conflict ... including the possibility that certain states will seek to deny others access to their maritime approaches'.[8] However, rather than providing direct analysis of the original source, he recycles Elinor Sloan's conclusion that a potential war with China seems to be the principal concern of the document, although summing up with the observation:

> [I]t seems doubtful that speculative security concerns about a country that has been embraced by the Canadian government as central to our trade and foreign policy can reasonably be used to justify spending billions of dollars on submarines.[9]

Of course, one might point out that *Horizon 2050*'s anti-access discussion is equally applicable to many other powers besides China. Submarines are a growing component of many navies' order of battle. In the last 20 years, almost every significant navy in the Asia Pacific has acquired submarines.[10] Russia continues to operate a sophisticated submarine force, one that has recommenced making regular visits to North American coasts.[11] India has entered the nuclear submarine community,[12] and yes, China's submarine fleet continues to grow.[13] It is not an enormous intellectual stretch to argue, as *Horizon 2050* does, that naval warfare in the 21st century will employ more sophisticated area denial capabilities using 'high-end' conventional or asymmetric capabilities, such as advanced missiles or submarines. If anything, the wide proliferation of submarine systems internationally speaks more to their continuing utility.

Arctic angst

The acquisition of the Victoria-class submarines from Britain was partly justified on the premise that they could be retro-fitted for air independent propulsion, making them suitable for under-ice operations in the high Arctic. This has been a capability the RCN has always desired.[14] An under-ice capability formed the justification for its futile quest to acquire nuclear submarines in the 1980s,[15] and it also has formed the basis for long-term cooperation with the US Navy in a series of secret operations conducted by American submarines in the Canadian Arctic throughout the Cold War.[16] As such, Byers suggests that without air independent propulsion, Canadian submarines are of little value in protecting the Arctic.

However, it is quite likely that the high Arctic will be increasingly ice-free in the coming decades. Shipping companies are expressing increasing optimism with respect to using polar trade routes to shorten the sailing distances between Asia and Europe, and many companies are eyeing the potential resources that may become exploitable in Arctic waters once year-round ice disappears. Canadians frequently forget that the Arctic is an ocean, one that is about to get considerably busier in the coming decades and one that is gathering increased attention by many major powers, China and Russia included.

The RCN has a real interest in monitoring activities in this region and submarines will play an important role. Even if they remain incapable of extended under-ice operations, access to the Arctic can be through waters that are largely ice-free, allowing the RCN to conduct barrier patrols of those chokepoints and enabling Canada greater visibility on the maritime and naval activities taking place in its Arctic waters.

Intelligence sharing and other naval cooperation

Byers argues that the exclusive submarine forums in which the RCN participates with its closest allies can be preserved in the absence of strict possession of these systems. While he speculates that essentially it would be in the interest of Canada's allies to continue to cooperate due to safety and search-and-rescue issues, he fails to understand that waterspace management is not about search-and-rescue but rather about route deconfliction. Allies participating in submarine waterspace management do not specifically reveal where each of their submarines are at any given moment. Waterspace management is all about the safe operation of submarines among friendly partners to ensure that their submarines do not collide with each other or are detected as unknown and potentially hostile targets.[17] Remove Canadian submarines from the game and there is no longer a 'need to know' basis for sharing information.

In terms of their most highly-guarded secrets, nations do not operate on the basis of charity. This was made dramatically evident to Canada in 2003 when its decision to abstain from the Iraq invasion caused the momentary loss of all military information sharing with the US.[18] New Zealand still feels the reverberations of its decision to ban US naval vessels from its ports in the 1980s. While the concept of 'need to share' has been in vogue since the events of 9/11, it has never been fully embraced, and information sharing—even in organisations such as NORAD (North American Aerospace Defense Command), where Canadian and American operations are completely integrated and command and control is shared—remains problematic.[19]

Even in terms of waterspace management, not all information is shared among allies, as the collision between HMS *Vanguard* and the French SSBN *Le Triomphant* demonstrates.[20] Further, Canada's decision to eschew offensive cyber capabilities for its armed forces has limited cyber cooperation with its close allies. Getting out of the submarine business would most certainly end any role for Canada in allied waterspace management.

Byers also dismisses Canadian naval cooperation with the US Navy as unnecessary, given that the US could find other NATO partners to conduct anti-submarine warfare training against conventional diesel-powered submarines. While this is undoubtedly true, it misses the whole point of why such training is conducted in the first place. The US benefits from training against Canada's conventional submarines but our navy, as well as air force, also gain significant benefits from these activities.

Canada's navy is rightly regarded as a world-class professional force, despite its small size. Such professionalism makes Canadian ships highly desired in multinational formations and has also allowed the RCN to lead those formations in many instances. International cooperation is a critical aspect of maintaining this level of world class professionalism. Furthermore, given the highly technical nature of submarine operations, working with American units is a key way to ensure that our submarine crews are every bit as good as their colleagues on the surface.

Surveillance and UAVs

Byers argues that 'as a result of technological developments, the surveillance of non-state actors can be done more effectively and efficiently with unmanned aerial vehicles (UAVs or "drones")', pointing to the Royal Canadian Air Forces' (RCAF) Justas program to acquire these types of aircraft.[21] It is true that such aircraft, on a vehicle-by-vehicle comparison, are dramatically less expensive than a submarine, and often less expensive than manned aircraft as well. However, the Justas program is nowhere near to fielding an operational capability for the RCAF. Further, with regards to the argument that UAVs can achieve the same effect as submarines, there are significant cost and capability issues in doing so.

First, maritime surveillance operations are those conducted at a distance, involving areas of thousands of square miles. In order to communicate with and control UAVs at these distances, some form of satellite communications is required. The infrastructure associated with this type of capability is neither easy to acquire nor cheap. For example, Great Britain's Royal Air Force (RAF) has been operating Reaper UAVs in Afghanistan since 2006. However, only recently has

the RAF been able to acquire its own command and control systems for its fleet of UAVs. In the meantime, it has had to use US Air Force facilities at Creech Air Force Base in Nevada.[22]

Second, significant modifications to Transport Canada's air safety regulations will have to be made in order to use UAVs in 'unsegregated airspace'.[23] While aircraft above 5000 feet are in controlled airspace, they all operate within a 'seek and avoid' paradigm with respect to other aircraft. With a pilot absent from the aircraft itself, the situational awareness of UAV pilots is significantly restricted. Furthermore, collision avoidance radars continue to experience developmental issues.[24] As such, save for over controlled military ranges, UAVs are currently banned from flying in both domestic and international airspace used by private and commercial aircraft, unless such flights are planned long in advance.

Last, there are presently few UAVs capable of flying in extreme weather conditions, such as frequently experienced in demanding environments off the coasts of Canada.[25] While the US Navy has stood up two squadrons of maritime surveillance UAVs, because they have undoubted utility, such systems are not inexpensive. The present system is based on the Global Hawk airframe, one of the most expensive UAV systems in operation.[26] In comparison to UAVs, submarines can remain effective and on station in the worst weather conditions.

Submarines in the contemporary strategic environment

Despite the continuous barrage of bad press, submarines remain a critical component of maritime capability. However, the debate over them sadly remains mired in narrow tactical considerations, rather than considering the broader strategic effects the technology offers. The future remains unpredictable and is unlikely to be orderly, and the Western liberal order established at the end of the Second World War is under increasing challenge by a variety of states.

Moreover, the threat of fragmentation through development of regional spheres of interest is a very real possibility. Russia's recent actions in the Crimea, and growing Chinese assertiveness in both the East and South China Seas, further point towards a world in which international governance may break down considerably and where the 'rules of the road' are set by the brute application of force rather than accommodation, negotiation and legal norms. Such a world is clearly not in Canada's interest. The defence of the liberal order, however, may ultimately require the use of force: the failure of it will certainly require it.

Clearly, Canada is not powerless in the contemporary strategic environment. The Canadian Government has seen fit to deploy its military forces in a variety of operations in support of both the UN and NATO since the end of the Cold War. In many of these operations, the geographic areas in which the Canadian Armed Forces (CAF) has taken action could hardly be called 'expected' or foreseeable.

As a wealthy, developed nation with interests in maintaining the present liberal governance structures of international society, Canada has seen fit to deploy its forces in Kosovo, Afghanistan and, most recently, Libya, in order to ensure that the values that underlie international society are protected from forces that seek to undermine and replace them with other forms of governance (either locally or globally). In committing forces to coalition and alliance operations, Canada has worked to protect (and project) liberal internationalist values, not only from hostile forces but also to influence its closest allies in terms of the interpretation of those values as they affect the conduct of operations.[27]

For a medium power, albeit still far removed from the sources of conflict, maintaining key military capabilities will be increasingly important for preserving Canadian freedom of action to influence this environment. Large military powers, such as the US, China and Russia, can afford to experiment with different forms of military structures. The size of their armed forces also gives them tremendous reserve capabilities to endure failures. While Canada deployed large, capable military forces in the First and Second World Wars, the cost of reacquiring such capabilities in the present environment would be enormous, and would require significant sacrifices to our existing social spending programs (and probably large tax increases as well).

For the foreseeable future, the size of the CAF is unlikely to grow. Canada will have to carefully husband its military power. Thus the employment of a fully capable navy, including the use of submarines, permits the Government of Canada to exercise both 'hard' and 'soft' power in a significant fashion with its allies, as well as against its enemies. In this, submarines offer tremendous flexibility to the Government of Canada as it determines the range of options it needs to pursue on the uncertain world stage.

We should consider, therefore, the following options that submarines offer to governments. Besides their ominous tactical offensive capabilities, three strategic roles fall naturally to submarines: strategic conventional deterrence, intelligence collection, and operational support.

Strategic conventional deterrence

Submarines are enormously difficult to find at sea. During the Second World War, the huge casualties suffered by German 'wolf packs' were partly caused by the speed of convoys that forced most submarines to attack on the surface, where ships and aircraft could more easily retaliate against them. However, modern submarines are much faster, which gives them the tactical manoeuvrability to attack while submerged.

As the Royal Navy found out in the Falklands War, modern anti-submarine warfare (ASW) is far trickier than in past conflicts. In 1982, Argentina effectively possessed a single submarine. Facing it were parts of NATO's North Atlantic ASW group, arguably one of the most experienced in the world. Despite its capability, the Argentinians were able to conduct two separate attacks on the British task force, albeit both failed because of torpedo malfunctions.[28] Local acoustic conditions, however, rendered British forces helpless: over 150 weapons were released with no hits against the Argentinian submarine *San Luis*. According to its captain, 'there was no effective counter attack. I don't think they knew we were there until they heard our torpedoes running',[29] the implication being that every ASW weapon expended by the British was against a false target.

Such operational difficulties exert a strong psychological effect. Knowledge of an operational submarine in a particular area will often deter navies from entering the area at all. Following the sinking of the *General Belgrano* by HMS *Conqueror*, the Argentinian Navy returned to port. However, such dramatic psychological effects can be created only by effective crews. The attack by the *San Luis* did not create the same impact as the successful attack by *Conqueror* because the Argentinians were not sufficiently capable from a technical perspective to prosecute an effective attack.[30] Key crewmen were absent in Germany and none of the command crew had any experience in the Type 209 submarine in which they were sailing.[31]

In a similar fashion to the effect created by *Conqueror*, the knowledge that the Canadian Navy had deployed submarines to the Georges Bank in 1995 assisted in managing the crisis between Spain and Canada during the so-called 'Turbot War' over disputed fisheries.[32]

Intelligence collection

The same features that enhance conventional deterrence also play an important role in intelligence collection. The ability to cruise undetected close to hostile shores demonstrates the utility of these vessels. During the height of the Cold War, American submarines were able to penetrate the ports of some of the Soviet Union's most sensitive naval installations, conducting signals and electronic intelligence, as well as photographing the undersides of Soviet submarines,[33] a standard to which Canadian crews also train.

Aside from such dangerous missions, they are also extremely effective assets in other operational contexts, complementing the intelligence resources available to a naval or ground force commander. Such missions might be able to collect intelligence unavailable by other means, especially the covert collection of signals and electronic intelligence. Opposing forces can avoid or deceive satellite reconnaissance as long as the orbital periods of space assets are known. Long-range, high-altitude aircraft, such as the U-2 and Global Hawk UAV, are highly scarce resources which may not be available on short notice. Furthermore, these and other aircraft may be detected, thereby warning the opposition that they are being watched.

A submarine's stealth avoids both these problems in maritime areas. No other platform has the ability to covertly track, identify and monitor vessels in the bad weather conditions that occur frequently off our coasts. 'Bottomed' submarines, resting on the sea floor, can conduct long range and long term intelligence operations in strategic waterways with little likelihood of being detected. Canadian submarines have been used for such purposes to monitor American fishing vessels thought to be illegally harvesting fish in Canadian waters,[34] and have supported counter-drug efforts in the Caribbean.[35] Having sovereign control over the collection and analysis of intelligence enhances Canadian decision making, especially during crises.

Operational support

Lastly, given the difficulty in finding and communicating with submerged submarines, they are rightly considered solitary weapon systems. However, in some circumstances, they can provide powerful operational support to other military systems. Under good sonar conditions, and when equipped with a towed array, a single submarine is capable of covering 125,000 square kilometres over a 40-50 day patrol, whereas a surface task group of five to six ships, with a combined helicopter capacity of eight aircraft, has a continuous surveillance coverage of 192,000 square kilometres in a 30-day patrol. Thus, considerable resource savings can be had with submarines, especially given that Canada's Victoria-class submarines have a core crew of 48 sailors, whereas a similarly capable naval task group might have as many as 1400 personnel, not to mention the considerable fuel costs, compared with that of a single submarine.[36]

Operating in conjunction with maritime patrol aircraft, submarines are able to assist in controlling enormous areas. Again, the sensors on board these vessels provide useful long-range information, although the submarine's ability to respond to that information may be limited by speed and safety considerations. Submarines operating with maritime patrol aircraft (or even, in the future, with organically-deployed UAVs)[37] can pass on their target information, allowing the aircraft to conduct more detailed investigations of contacts that are far removed from the submarine's position. This also has the benefit of allowing the submarine to remain covert. In this, Canadian operations in support of Operation CARIBBE, as well as Dutch operations in support of the NATO Operation OCEAN SHIELD, off the coast of Somalia, are both excellent demonstrations of how submarines can support surface forces.[38]

Conclusion

Those arguing that submarines have no use in a Canadian context are thinking in very narrow terms about what types of threats they can imagine, given the current political environment and how military force might be employed in the future. Our military contributions to Canadian security, whether exercised in terms of domestic operations or those in alliance, coalition or UN operations should be determined by our values and interests, rather than the availability of specific military capabilities.[39] Those who rely on the 'capability argument' avoid the difficult question of for what, as a country, we are willing—and occasionally need—to fight.

Clearly, as history since 1991 has shown, there are some things that even the most war-averse government has deemed necessary to support with military force.[40] What those issues will be in the future is entirely unknowable, just as it was impossible to imagine the high-intensity operations conducted by the Canadian Army in Kandahar province in 2006-07, or the bombing operations undertaken by the RCAF over Libya in 2010. Submarines offer tremendous flexibility with respect to how they can be used. While their acquisition costs are high (and their complex safety requirements make maintenance issues pricey), once acquired, their operational costs can be quite low.

As Yogi Berra famously observed, 'the future ain't what it used to be'. Russia appears to have made a fundamental determination that it cannot pursue its interests within the present liberal order. China also appears to be indicating that it seeks to challenge liberal norms that underlie international governance, as its actions in both the East and South China seas indicate. It seems unlikely that either state will pose the type of 'full spectrum' threat to international order that both Nazi Germany and the Soviet Union historically represented. But Russia and China, along with a host of minor military actors such as Iran, North Korea, Venezuela, Syria and others, can

easily play the role of 'spoilers' in a process some have referred to as 'lawfare', eroding the legal rules, norms and values that help to keep international relations peaceful and restrained.[41]

Canada's regional environment will be locally unaffected by many of these actions and, hence, Canadians have some amount of discretion as to whether they participate in future military operations that seek to support and enforce these liberal norms. Unlike those states immediately threatened by geographic proximity to aggression, Canada can choose to leave the hard work of protecting international society to others. Such a decision, however, would be in keeping with neither our traditions nor our interests.

As a wealthy Western state, Canada should bear a certain responsibility to protect an international order from which, as a power with limited military means at our immediate disposal, we greatly benefit. It is not in our interests to see that order eroded to the point that instability abroad begins to affect our local peaceful environment. In this effort, submarines can play a critical role for robust military response. Further, despite their recent problematic nature, they can do so in a far more economical and discreet fashion than many other forms of military power. It would be a mistake to conclude otherwise.

Paul Mitchell holds a Bachelor of Arts (Honours) from Wilfred Laurier University, a Master of Arts in War Studies from King's College London, and a PhD from Queen's University at Kingston. Following the completion of his doctoral studies, he worked as a post-doctoral fellow at Dalhousie University in Halifax in the Centre for Foreign Policy Studies.

He also worked as Directing Staff at the Pearson Peacekeeping Centre on its Maritime Peacekeeping course in 1996 and 1997. He has worked at the Canadian Forces College since 1998, first as the Deputy Director Academics, and later as its first Director of Academics.

Between 2005 and 2007, he was an Associate Professor at the S. Rajaratnam School of International Studies, Nanyang Technological University in Singapore, and also taught at the Singapore Armed Forces Training Institute's Command and Staff College. He is currently a Professor in the Department of Defence Studies at the Canadian Forces College.

ACKNOWLEDGEMENT AND DISCLAIMER

The author gratefully acknowledges the assistance of Vice Admiral Dean McFadden, RCN (Ret'd), Commodore Lawrence Hickey, RCN (Ret'd), Commander Scott McVicar, RCN, and Lieutenant Commander Tony March, RCN, as well as other officers who have chosen to remain anonymous.

The opinions expressed in this article are those of the author, and do not represent those of the Canadian Forces College or the Department of National Defence. Any errors or omissions are the responsibility of the author alone.

NOTES

[1] This is an edited version of an article by the author, published in the *Canadian Military Journal*, Vol. 14, No. 3, Summer 2014, pp. 15-25. It is reprinted with permission of the *Canadian Military Journal*.

[2] 'East Coast's only Working Submarine Going in for Generator Repairs', *The Globe and Mail*, 5 February 2014, available at <http://www.theglobeandmail.com/news/national/east-coasts-only-working-submarine-going-in-for-generator-repairs/article16723023/>

[3] Gervais Gamache, 'Atlantic Region News - *HMCS Toronto*: gas turbine replacement in the Persian Gulf', available at <http://www.navy-marine.forces.gc.ca/en/news-operations/news-view.page?doc=hmcs-toronto-gas-turbine-replacement-in-the-persian-gulf/hr0e3ova>; 'Fire-damaged *HMCS Protecteur* Could be Headed for the Scrap Heap', *National Post*, 4 March 2014, available at <http://news.nationalpost.com/2014/03/04/fire-damaged-hmcs-protecteur-could-be-headed-for-the-scrap-heap/>

[4] Michael Byers, 'Does Canada Need Submarines', *Canadian Military Journal*, Vol. 14, No. 3, Summer 2014, pp. 7-14, available at <http://www.journal.forces.gc.ca/vol14/no3/page7-eng.asp>

[5] Paul T. Mitchell, *Full of Holes: Byers and Webb on Canada's submarine programme*, Canadian Defence and Foreign Affairs Institute: Calgary, 2013, pp. 4-5.

[6] Only four *Upholders* were built when the RN divested itself of them. There is considerable commonality between the *Trafalgar* and *Victoria* classes. However, some differences exist, especially since Canada has conducted extensive modifications to the boats. Moreover, the spares the RN held were not fully acquired by the RCN, due to strict limits placed upon the cost of the program. Re-establishing these supplier networks has proven both expensive and challenging for the RCN.

[7] 'Exclusive Glimpse Behind the Scenes of the Royal Navy's Grueling Submarine Command Course Known as Perisher', *Daily Record*, 12 October 2013, available at <http://www.dailyrecord.co.uk/news/exclusive-glimpse-behind-scenes-royal-2364670>. The BBC has produced a television program on the course, available on YouTube, at <http://www.youtube.com/results?search_query=BBC+Perisher>

[8] Quoted in Elinor Sloan, 'US-China Military and Security Developments: implications for Canada', *International Journal*, Issue 66, Summer 2011, pp. 265-83.

[9] Byers, 'Does Canada Need Submarines', p. 8.

[10] Koh Swee Lean Collin, 'Submarines in Southeast Asia: proliferation, not an arms race', *The Diplomat*, 30 January 2014, available at <http://thediplomat.com/2014/01/submarines-in-southeast-asia-proliferation-not-a-race/>

[11] Phillip P. Pan, 'Russian General Calls Submarine Patrols off US East Coast Routine', *The Washington Post*, 6 August 2009, available at <http://www.washingtonpost.com/wp-dyn/content/article/2009/08/04/AR2009080402863.html>; 'Russian Attack Sub Discovered Just 200 Miles from US East Coast is Given Safe Harbor During Hurricane *Sandy', Daily Mail Reporter*, 6 November 2012, available at <http://www.dailymail.co.uk/news/article-2228487/Russian-attack-sub-discovered-just-200-miles-East-Coast-given-safe-harbor-Hurricane-Sandy.html>

[12] Rajat Pandit, 'India's First Nuclear Submarine and ICBM will be Ready for Induction Next Year: DRDO', *The Times of India*, 8 February 2014, available at <http://timesofindia.indiatimes.com/india/Indias-first-nuclear-submarine-and-ICBM-will-be-ready-for-induction-next-year-DRDO/articleshow/30019630.cms>

[13] Zachary Keck, 'Russia May Sell China New Advanced Submarines', *The Diplomat*, 28 March 2014, available at <http://thediplomat.com/2014/03/russia-may-sell-china-new-advanced-submarines/>; Owen R. Cote Jr., 'Assessing the Undersea Balance Between the US and China', *MIT Security Studies Program Working Paper*, February 2011, available at <http://web.mit.edu/ssp/publications/working_papers/Undersea%20Balance%20WP11-1.pdf>

[14] Douglas Bland, 'Continuity in Canadian Naval Policy, 1961-1987', *Canadian Defence Quarterly*, April 1989.

[15] Julie H. Ferguson. *Through a Canadian Periscope: the story of the Canadian Submarine Service*, Dundurn Press: Toronto, 1995, p. 301.

[16] Adam Lajeunesse, 'A Very Practical Requirement: under-ice operations in the Canadian Arctic, 1960-1986', *Cold War History*, Vol. 13, No. 4, 2013, available at <http://www.tandfonline.com/doi/abs/10.1080/14682745.2012.727800#.Ub9todgmydn>

[17] Phil Webster, 'Artic Sovereignty, Submarine Operations, and Water Space Management', *Canadian Naval Review*, Vol. 3, No. 3, Fall 2007, available at <http://www.navalreview.ca/wp-content/uploads/public/vol3num3/vol3num3art4.pdf>

[18] Paul T. Mitchell, *Network Centric Warfare and Coalition Operations in an Age of US Military Primacy*, Adelphi Paper #385, Taylor and Francis: London, 2006.

[19] Paul T. Mitchell, *Network Centric Warfare and Coalition Operations: the new military operating system*, Routledge: Abingdon, 2009, pp. 68-96; Richard A. Best Jr., *Intelligence Information: need-to-know vs. need-to-share,* Congressional Research Service: Washington DC, 6 June 2011, available at <http://www.fas.org/sgp/crs/intel/R41848.pdf>

[20] Richard Norton Taylor, 'Two Subs, Dozens of Nuclear Warheads, One Huge Ocean - and a Stroke of Bad Luck', *The Guardian*, 17 February 2009, available at <http://www.theguardian.com/uk/2009/feb/17/nuclear-submarine-collision>; 'French and UK May Coordinate Submarine Patrols', *Die Welt*, 2 February 2009, available at <http://www.welt.de/english-news/article3220555/French-and-UK-may-coordinate-submarine-patrols.html>

[21] Byers, 'Does Canada Need Submarines', p. 12.

[22] 'RAF Reaper Drone Squadron Stood up at RAF Waddington', *BBC News*, 23 October 2012, available at <http://www.bbc.com/news/uk-england-20039085>

[23] J.S.F. LaPlante, 'The Use of Unmanned Aerial Systems in Canada's Unsegregated Airspace: foundations and roadmap', Masters of Defence paper, Canadian Forces College, 2013, pp. 16, 43-5.

[24] Bill Carey, 'Navy Rethinks Sense-and-Avoid Radar on MQ-4C', *Aviation International News*, 16 August 2013, available at <http://ainonline.com/aviation-news/ain-defense-perspective/2013-08-16/navy-rethinks-sense-and-avoid-radar-mq-4c>

[25] Jason Kenny, 'Unmanned Aerial Systems: are expectations realistic*?',* Masters of Defence paper, Canadian Forces College, 2012, pp. 30-54. See also 'UAV Not Best Choice For Finding Boats', *UAS News*, available at <http://www.suasnews.com/2013/07/23637/uav-not-best-choice-for-finding-boats/>

[26] 'MQ-4C Triton Broad Area Maritime Surveillance (BAMS) UAS, United States of America', available at <http://www.naval-technology.com/projects/mq-4c-triton-bams-uas-us/>. See also Sharon Weinberger, 'Meet Triton, the Navy's New Spy Drone', *Popular Mechanics*, 14 June 2012, available at <http://www.popularmechanics.com/technology/military/planes-uavs/meet-triton-the-navys-new-spy-drone-9718704>

[27] As Commodore Eric Lerhe (Ret'd) has demonstrated, legal officers from the CAF were able to shift American detainee policy away from unilateralist interpretations of the Geneva Conventions and towards a more internationalist interpretation of that code. Eric Lerhe, *At What Cost Sovereignty: Canada-US military interoperability in the War on Terror*, Centre for Foreign Policy Studies: Halifax, 2013, pp. 159-206.

[28] See <http://www.navy-net.co.uk/submariners/41067-1982-attacks-rn-ara-san-luis-5.html> for an excellent technical discussion of the ARA *San Luis*'s attack on the British task group.

[29] Quoted in Christopher McConnaughy, 'China's Emerging Military Doctrine: a role for nuclear submarines' in Andrew Erikson, Lyle Goldstein, William Murray and Andrew Wilson, *China's Future Naval Submarine Force*, China Maritime Studies Institute and Naval Institute Press: Annapolis, 2007, p. 95.

[30] The most experienced Argentinian crewmen were in Germany at the time of the war, supervising the construction of new submarines.

[31] Furthermore, the submarine's fire control system was inoperable and the crew was unable to repair it, limiting the submarine to a single manually controlled torpedo shot on each attack run.

[32] Canada issued a 'Submarine Notice of Intention' in the spring of 1995, advertising an area where submarines would be operating as a way of communicating to the Spanish the presence of a Canadian submarine. Webster, 'Artic Sovereignty, Submarine Operations, and Water Space Management', p. 33.

33 Sherry Sontag and Christopher Drew, *Blind Man's Bluff: the untold story of American submarine espionage*, Harper Collins: New York, 1999.

34 Sean M. Maloney, 'Canadian Subs Protect Fisheries', *Proceedings*, Vol. 124, No. 3, March 1998, available at <http://www.usni.org/magazines/proceedings/1998-03/canadian-subs-protect-fisheries>. See also Laurence M. Hickey, 'The Submarine as a Tool of Maritime Enforcement', *Integrated Coastal Zone Management*, Spring 2000, pp. 117-22.

35 David Pugliese, 'Op Caribbe 2013 Wraps Up – *Her Majesty's Canadian Ships Edmonton* and *Yellowknife* and *HMC Submarine Victoria* Complete Deployments In Eastern Pacific Ocean', *Ottawa Citizen*, 17 December 2013, available at <http://blogs.ottawacitizen.com/2013/12/17/op-caribbe-2013-wraps-up-her-majestys-canadian-ships-edmonton-and-yellowknife-hmc-submarine-victoria-complete-deployments-in-eastern-pacific-ocean/>

36 Canadian submarines frequently sail with a crew complement in excess of 50 sailors. Commander Michael Craven observes: 'By way of example, the steady-state cost of ownership of the four-boat *Victoria* fleet is estimated at about $C250 million per year, with an 'all up' personnel requirement, including support staff ashore, of less than 500 people. Comparatively, a non-nuclear submarine costs some 30 per cent less than a frigate or destroyer to keep at sea on a daily basis, in part the consequence of smaller crew and greater fuel economy': Michael Craven, 'A Rationality Choice Revisited: submarine capability in a transformational era', *Canadian Military Review*, Vol. 7, No. 4, 2008, available at <http://www.journal.forces.gc.ca/vo7/no4/craven-eng.asp>.

37 Owen R. Cote Jr., 'Submarines in the Air-Sea Battle', MIT Security Studies Program Working Paper, 2010, available at <http://web.mit.edu/ssp/publications/conf_reports/3coteorPAD3.pdf>

38 'Dutch submarine to help NATO combat piracy off Somali coast', *NATO News*, 28 June 2010, available at <http://www.nato.int/cps/en/natolive/news_64706.htm>

39 James Fergusson, 'The right debate: airpower, the future of war, Canadian strategic interests, and the JSF decision', *Canadian Foreign Policy Journal*, Vol. 13, No. 3, 2011, p. 214.

40 Joseph Jockel and Joel Sokolsky, 'Lloyd Axworthy's Legacy: human security and the rescue of Canadian defence policy', *International Journal*, Vol. 56, No. 1, Winter 2000.

41 Charles J. Dunlap, Jr., 'Law and Military Interventions: preserving humanitarian values in 21st century conflicts', available at <http://people.duke.edu/~pfeaver/dunlap.pdf>; also speech delivered by Brooke Goldstein, 'Lawfare: real threat or illusion', available at <http://www.thelawfareproject.org/Articles-by-LP-Staff/lawfare-real-threat-or-illusion.html>

Improving the Australia-New Zealand Defence Relationship [1]

Group Captain Matt Hegarty, Royal Australian Air Force

Introduction

The strong relationship between Australia and New Zealand arises from their shared historical beginnings, common values and institutions, and significant people-to-people links.[2] As a consequence, the two nations have extensive bilateral relations that are supported by annual Prime Ministers' meetings, and regular bilateral meetings between their respective Foreign, Trade and Defence Ministers.[3] The defence relationship is particularly strong, with its roots in the Gallipoli campaign of World War 1, and evident in all of the major wars of the 20th century which Australia and New Zealand have fought in together.[4]

The formal security treaties that bind Australia and New Zealand are the 1944 Canberra Pact and the 1951 ANZUS Treaty, the latter a trilateral alliance with the US.[5] In addition to the formal security alliances, the Australia and New Zealand defence relationship is very much strengthened by the Closer Defence Relations Agreement (CDR), signed in 1991 and revised in 2003 and 2008.[6] A key objective is 'collaboration of defence activities that support the development of interoperability'.[7] Adding to the suite of defence agreements is the joint 2011 Review of the Australia-New Zealand Defence Relationship, which calls for 'improve[d] bilateral engagement structures, strengthen[ed] strategic exchanges' and efforts to improve acquisition and operating efficiencies.[8]

Yet despite this comprehensive accumulation of defence-related agreements, there remain many areas where greater efficiency and improved capability and interoperability can be achieved.[9] This article examines the drivers for strengthening Australia-New Zealand defence relations and selects strategic air transport as one area for deepening engagement, proposing three options to improve both efficiency and effectiveness.

The impetus for strengthened defence relations

The defence policies of Australia and New Zealand are explicit in their support for the other nation, recognising their shared values and perspectives on regional security. Australia's 2013 *Defence White Paper* asserts that 'Australia and New Zealand share a close defence relationship, reinforced by common strategic and security interests in the South Pacific', noting that Australia would most likely partner with New Zealand in dealing with regional issues.[10] New Zealand's 2010 *Defence White Paper* notes as a number two priority the need to be able to discharge alliance obligations to Australia, and to be able to deal with contingencies in the South Pacific in partnership with Australia.[11] Both policies infer the need for partnerships enabled through interoperability.

Australia's *Defence White Paper* and the 2011 joint review discuss strategic and security issues common to Australia and New Zealand and both highlight the constraints on the funding available to their respective defence forces.[12] Of significance, the 2011 review notes the need to 'take full advantage of existing and potential future complementarities to reduce or eliminate potential capability gaps'.[13]

New Zealand's *Defence White Paper* notes that the New Zealand Defence Force's (NZDF) share of GDP fell from 1.7 per cent in 1990 to 1.0 per cent in 2009 and is forthright in noting the unaffordability of modern 'high-end' military capabilities.[14] In Chapter 2, New Zealand's broad understanding and intent with respect to the defence relationship with Australia is declared:

> New Zealand's own security is enhanced by the investment which Australia has made in its national defence. Australia has military capabilities that we do not have, but which are essential for higher-end contingencies. The ANZAC relationship enhances the overall depth and reach of the NZDF. It is therefore in our interest to add to Australia's strategic weight.[15]

The conclusion to be drawn is that not only are both countries looking to deepen the defence relationship because of close friendships and shared values but that they also seek to leverage the strengths of each defence force to maximise the strategic effect sought in the pursuit of common goals.

The Ministers of Defence of both Australia and New Zealand endorsed the recommendations of the 2011 review in January 2012.[16] At the annual bilateral Defence Ministers' meeting in November 2012, they agreed to a range of measures to deepen the relationship, including mutual sealift cooperation and cross-crewing of navy platforms, working towards the inclusion of New Zealand in the biennial Australia/US Exercise TALISMAN SABRE in 2015 and additional personnel exchanges.[17]

In the December 2013 meeting between the two Ministers, these measures were reaffirmed but little else was added despite the imperatives outlined in the 2011 review and the continuing pressures on their respective national budgets.[18] However, it is clear that more can be done and one area hinted at in both nations' defence policies is air transport.

New Zealand and Australian strategic air transport capability

The New Zealand *Defence Capability Plan* notes the critical importance of strategic air transport but also notes that New Zealand's two strategic air platform types—five 're-lifed' C-130H Hercules and two B-757 airliners—will need replacing in the 2018-25 timeframe.[19] In contrast, Australia's air transport fleet is quite young. Australia operates 12 C-130J, six C-17A, five KC-30A and, from 2015, will introduce the first of ten C-27J.[20] This combination of mostly new, medium and heavy airlifters contrasts starkly with New Zealand's ageing fleet. A joint Australia-New Zealand approach to military air transport, which leverages complementarities and reduces capability gaps has great potential for improved bilateral defence relations.

The 2013 Australian *Defence White Paper* notes that 'recent initiatives to facilitate … air lift coordination [with New Zealand] will remain a priority'.[21] One of those initiatives is a memorandum of agreement between the UK, New Zealand and Australia, titled Air Transport and Air Refuelling Exchange of Services (ATARES), which establishes the procedures by which participants can exchange air transport and air-to-air refuelling.[22]

The agreement has already been put to some good use by Australia and New Zealand using cargo space and passenger seats on each other's aircraft for a range of mission types. The Australian Defence College, for example, has used a RNZAF B-757 in 2013 and 2014 to transport the Defence and Strategic Studies Course on field research visits to Northeast Asia. Similarly, New Zealand has made frequent use of the ADF's chartered A-340 aircraft moving Australian Defence personnel and cargo to and from the Middle East and, on several occasions, has utilised the very large cargo capacity offered by the RAAF's C-17.

However, the system requires participants to search for tasking opportunities rather than the system automatically coordinating the most efficient and effective use of the total asset pool, meaning that much opportunity is wasted. But there are at least three examples where increasingly more efficient and effective, but also more complex, frameworks exist in the European theatre.

Opportunities and options

The first example is the Movement Coordination Centre Europe (MCCE), an international military movements control centre, whose 25 member states are from the EU and NATO. Its mission is to:

> Coordinate participants' strategic lift (air, sea and inland surface transport) and air-to-air refuelling [AAR] capabilities with operational, exercise and routine requirements for lift and AAR in order to improve efficiency and effectiveness through identifying available assets, advertising these assets and then coordinating their use to the maximum extent possible.[23]

The Air Transport Cell, a sub-component of the MCCE, coordinates airlift requests by participating nations, matching loads to spare capacities given up by other participating nations. The essential difference between the ATARES agreement and the MCCE is that the latter is a permanent, coordinating body staffed by nationals of the participating nations. Matching loads to spare capacity is, therefore, an everyday, routine activity rather than the *ad hoc* arrangement currently existing between Australia, New Zealand and the UK.

For Australia and New Zealand to create a similar arrangement, both nations would ideally co-locate existing movements functions in an existing work place. A coordination centre, separate to both national movements organisations, would unnecessarily duplicate functions at considerable cost of workforce.[24] The same concept could be applied to the coordination of land and sea movements, which the respective 'Joint Movements' organisations in both nations could also adopt.

The second example is the European Air Transport Command (EATC), where the Netherlands, Belgium, France, Germany and Spain have placed large proportions of their respective air transport fleets under a unified operational command. Within EATC:

> [T]he missions of almost 150 aircraft are planned, tasked and controlled…. In addition to that the EATC runs a nationally defined level of responsibility for aircrew training, coordination of training and exercise objectives as well as the harmonization of appropriate air transport regulations of the participating nations. The overall objective is to manage the scarce resource air transport as effectively and efficiently as possible.[25]

The EATC concept is a significant leap in the achievement of effectiveness and efficiency over the MCCE model because the planning and tasking of air transport assets is controlled by a central agency responsible for ensuring maximised efficiency rather than simply coordinating loads with space declared available at the generosity of a donor. To replicate such a model, Australia and New Zealand would need to create a common control centre or integrate a combined cell within an existing air tasking control centre, and assign air assets to a common command. In practice, aircraft operating units would be assigned tasking from the combined cell in accordance with previously-agreed obligations and operate otherwise as normal.

The third example goes even further in achieving outcomes for the participants that would not otherwise be available to them individually. The Strategic Airlift Capability (SAC) is a group of 12 NATO and European participating nations that jointly own and operate three Boeing C-17 aircraft.[26] The aircraft are registered, flagged and based in Hungary but members from all the participating nations staff the operating unit.[27]

The most significant benefit from this arrangement is the ability of nations of lesser means to buy a portion of an otherwise unobtainable operating capability they might need only infrequently. In the case of Australia and New Zealand, a similar outcome could be achieved if New Zealand was to 'buy into' the existing Australian C-17 squadron by contributing financially or to the workforce and, potentially, assisting in the purchase of additional aircraft to augment the existing six.

For and against

The MCCE and EATC models offer increased load capacity utilisation and a broader set of capability options. Moreover, during operational surges, both models offer the ability to move greater loads more quickly. In the case of the SAC heavy airlift model, the combined (joint nation) capability offers New Zealand an opportunity to own part of a very expensive but very capable heavy airlift capability not otherwise obtainable. For Australia, the model potentially adds additional aircraft and increased capability through shared operating costs and additional workforce.

Key among the downsides for all models are sovereignty concerns although, for the MCCE and EATC models, these concerns can be avoided (at the expense of effectiveness) by strict adherence to individual national requirements. The application of such constraints is not new and has been incorporated in multinational efforts previously, such as in Afghanistan and Timor.

The SAC model, however, does present some unique challenges, including the application of diplomatic clearance procedures where, for example, an aircraft is crewed by and on behalf of one state when the aircraft is registered as a state aircraft of another. An additional obstacle potentially exists in the form of US Government International Trade in Arms Restrictions, noting that Australia currently has approval to operate the C-17 and New Zealand does not. However, recent improvements in defence relations between New Zealand and the US suggest that such restrictions might be readily navigated should a model like the SAC be pursued.[28]

Conclusion

This article has examined the drivers behind the call for improvements to the defence relationship between Australia and New Zealand. Those drivers are to be found in the Defence White Papers of both nations and the 2011 joint review. Key among them is the need to 'train, operate and deliver engagement programmes in a more coordinated fashion'.[29] The article has argued that one area that can be readily improved is air transport coordination.

While air transport is only a small part of the broader Australia-New Zealand defence relationship, the air transport capability is of strategic significance, as recent operations in East Timor, Fiji and the Solomon Islands have demonstrated. Constrained defence budgets are good reasons for pursuing one or more of the possible models but, more importantly, improved air transport effectiveness offers Australia greater interoperability with its closest security partner in the South Pacific. For New Zealand, the opportunity exists to greatly improve its air mobility and hedge against the potential shortfall in the coming decade.

Group Captain Matt Hegarty joined ADFA in 1988 and, after graduating, commenced pilot training in 1991 at RAAF Base Point Cook. His early postings included flying C-130E Hercules at No. 37 Squadron, Aide-de-Camp to the Air Officer Commanding at Headquarters Logistics Command, flying the C-130H at No. 36 Squadron, and a staff position at Headquarters Air Lift Group.

After attending the Australian Command and Staff Course in 2005, his postings included Executive Officer in No. 86 Wing, command of No. 37 Squadron, and a staff position in the Air Force Personnel Directorate. In April 2011, he was posted on promotion as Director of the KC-30A Transition Team. Group Captain Hegarty has completed two operational deployments to the Middle East. He has a Masters of Management in Defence Studies (University of Canberra) and is currently attending the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College.

NOTES

1 This is an edited version of a paper developed by the author while attending the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College in 2014.

2 New Zealand Ministry of Foreign Affairs and Trade's website, available at <http://www.mfat.govt.nz/Foreign-Relations/Australia/index.php> accessed 28 August 2014.

3 Australian Department of Foreign Affairs and Trade (DFAT), *New Zealand Country Brief*, DFAT website, available at <https://www.dfat.gov.au/geo/new_zealand/nz_country_brief.html> accessed 5 August 2014.

4 New Zealand Ministry of Foreign Affairs and Trade's website.

5 DFAT, *New Zealand Country Brief.*

6 The New Zealand Government's anti-nuclear stance resulted in the suspension of the security obligations between the US and New Zealand under ANZUS in 1986, however the relationship between Australia and New Zealand remained firm and was possibly strengthened as a result. See Robert Ayson, 'When Cooperation Trumps Convergence: emerging trends in Australia-New Zealand defence relations', *Security Challenges*, Vol. 2, No. 3, October 2006, p. 31.

7 Jon Grevatt, 'Australia, New Zealand to enhance procurement and R&D collaboration', *Jane's Defence Weekly*, 30 January 2012.

8 Australian Department of Defence, New Zealand Ministry of Defence, 'Review of the Australia-New Zealand Defence Relationship', available at <http://www.defence.gov.au/review/ausnzrelationship/docs/Joint%20Report%20on%20AS-NZ%20Review.pdf> accessed 5 August 2014. The Departments of Defence of both nations prepared the 2011 review and report jointly.

9 Australian Department of Defence, New Zealand Ministry of Defence, 'Review of the Australia-New Zealand Defence Relationship', pp. 2-3.

10 Australian Government, *Defence White Paper 2013*, Department of Defence: Canberra, 2013, p. 63.

11 New Zealand Government, *Defence White Paper 2010*, Ministry of Defence: Wellington, November 2010, pp. 11 and 37.

12 Australian Government, *Defence White Paper 2013*, p. 63.

13 Australian Department of Defence, New Zealand Ministry of Defence, 'Review of the Australia-New Zealand Defence Relationship', p. 3

14 New Zealand Government, *Defence White Paper 2010*, p. 47.

15 New Zealand Government, *Defence White Paper 2010*, p. 18.

16 Department of Defence, 'Minister for Defence – Australia and New Zealand release bilateral Defence Framework', press release, 24 April 2012, available at <http://www.minister.defence.gov.au/2012/04/24/australia-and-new-zealand-release-bilateral-defence-framework/> accessed 17 August 2014.

17 Department of Defence, 'Minister for Defence – Joint Media Release – Australian and New Zealand Defence Ministers boost ANZAC Defence cooperation', Australian Government, press release, 16 November 2012, available at <http://www.minister.defence.gov.au/2012/11/16/minister-for-defence-joint-media-release-australian-and-new-zealand-defence-ministers-boost-anzac-defence-cooperation/> accessed 17 August 2014.

18 Department of Defence, 'Minister for Defence and New Zealand Minister for Defence – Defence Ministers reaffirm commitment to bilateral defence relations', press release, 18 December 2013, available at <http://www.minister.defence.gov.au/2013/12/18/minister-for-defence-and-new-zealand-minister-for-defence-defence-ministers-reaffirm-commitment-to-bilateral-defence-relations/> accessed 23 August 2014.

19 New Zealand Government, *Defence Capability Plan,* Ministry of Defence: Wellington, June 2014, available at <http://www.defence.govt.nz/pdfs/reports-publications/defence-capability-plan-2014.pdf> accessed 23 August 2014, p. 34.

[20] Australia's oldest platform is the C-130J, which was introduced in the 1999/2000 period. Complementing these 12 medium airlifters are six C-17A heavy airlifters, introduced from 2007, and five Airbus A330 derivative KC-30A (multi role tanker transport) aircraft introduced in 2011/12.

[21] Australian Government, *Defence White Paper 2013*, p. 63.

[22] The author obtained a copy of the memorandum from within Air Force. Although it is unclassified, it seems not to be in the public domain.

[23] Movement Coordination Centre Europe's website, available at <https://www.mcce-mil.com/Pages/default.aspx> accessed 21 August 2014. Of particular note is that MCCE coordinates air, land and sea transport across the participating nations.

[24] An internal US Transportation Command (USTRANSCOM) brief written in July 2013 recommended that USTRANSCOM should pursue the creation of a movement coordination centre in the Pacific (MCC-P) and invite nations such as South Korea, Japan, Australia and ASEAN members. While not specifically mentioned, New Zealand would almost certainly be welcomed. The brief was made available by the ADF's Headquarters Joint Operations Command.

[25] European Air Transport Command's website, available at <http://eatc-mil.com> accessed 28 July 2014.

[26] The SAC partners consist of 10 NATO nations: Hungary, Bulgaria, Estonia, Lithuania, the Netherlands, Norway, Poland, Romania, Slovenia, US and two NATO 'Partnership for Peace' nations, Sweden and Finland.

[27] Strategic Airlift Capability Heavy Airlift Wing's website, 'About the Strategic Airlift Capability Heavy Airlift Wing', available at <http://www.heavyairliftwing.org/about/faq> accessed 28 July 2014.

[28] In November 2010, the US Secretary of State and New Zealand Minister for Foreign Affairs signed the Wellington Declaration outlining a new strategic partnership. In June 2012, New Zealand Minister for Defence and the US Secretary of Defense signed the Washington Declaration outlining US-New Zealand Defence Cooperation initiatives. See Robert Ayson and David Capie, 'Part of the Pivot? The Washington Declaration and US-NZ Relations', *Asia Pacific Bulletin*, East-West Centre, No. 172, 17 July 2012.

[29] Australian Department of Defence, New Zealand Ministry of Defence, 'Review of the Australia-New Zealand Defence Relationship', p. 4.

Challenging the Myths about Flexible Work in the ADF

Associate Professor Abby Cathcart, Queensland University of Technology
Professor Paula McDonald, Queensland University of Technology, and
Dr Deanna Grant-Smith, Queensland University of Technology

Introduction

In May 2011, the Minister for Defence requested a review into the treatment of women in the ADF following allegations of inappropriate conduct at the Australian Defence Force Academy. The Australian Human Rights Commission (AHRC) initiated the review under the leadership of the Federal Sex Discrimination Commissioner, Elizabeth Broderick, who challenged the ADF to improve its culture and build a more inclusive environment for its members.

The need for flexible work arrangements (FWAs) emerged as a central issue in the review, not least as a mechanism for improving the recruitment and retention of women in the ADF. The review, and its subsequent audit report, concluded that flexibility would strengthen the ADF but that there were cultural and structural obstacles.[1]

This article addresses the uptake of formal and informal FWAs in the ADF. The study is part of an Australian Research Council funded project, led by Queensland University of Technology, which addresses how the timing, location and tasks of work are negotiated in exchanges between managers and employees.

This phase of the project, supported by the ADF, explored the experiences of Defence personnel in customising the terms and conditions of their work. The project involved interviews with personnel in the three Services across Australia. The uptake of FWAs was defined as situations where an employee formally or informally requests or negotiates with their supervisor to adjust the 'standard' terms and conditions of their work. The results reveal the types and frequency of requests for FWAs made by these ADF members and the extent to which these requests were approved, partly approved or declined.

Defence policy on FWAs is detailed in the *Military Personnel Policy Manual*, supported by various *Defence Instructions*.[2] SUAKIN, a major ADF workplace reform project, was launched in November 2013 with the aim of introducing a range of full-time, part-time and casual employment categories designed to offer members more employment flexibility.[3] In conjunction with the SUAKIN reforms, significant revisions have been made, with the current policy outlining five forms of FWAs (see Table 1).

Table 1: **Forms of flexible work arrangements available to Defence members**

Form	Abbreviation	Purpose
Home-located work	HLW	To enable a Defence member to work at a specified location outside of the normal workplace, on an occasional, temporary or ongoing basis.
Variable working hours	VWH	To enable a Defence member to vary their start and finish times, and periods of absence to suit their individual circumstances on a one-off or ongoing basis.

Form	Abbreviation	Purpose
Part-time leave without pay	PTLWOP	To enable a Defence member to maintain continuity of service although working a reduced number of days or part days in each fortnight. Minimum period of 3 months.
Alternate located work	ALW	To enable a Defence member to work from an alternate location outside of a posting location, such as another Defence Base on a temporary, occasional or ongoing basis.
Remote overseas work	ROW	To enable a Defence member to undertake work while living and residing overseas, generally on a long-term enduring basis where a member is accompanying a spouse or partner overseas.

In 2014, the AHRC recommended that each Service Chief agree an annual growth target for FWAs with the CDF, and that progress against the target be reported annually. The ADF consequently set a 2 per cent target for the uptake of formal FWAs across all trained forces by December 2014, and has committed to taking a tri-Service approach to centralising data and policy on FWAs.[4]

To date, data collected by the ADF on the use of FWAs is limited, and it remains unclear precisely how many members were using the various forms of FWAs prior to the 2 per cent target being set. However, the 2011 *Department of Defence Census* indicated that 1 per cent of ADF personnel were serving part-time, and the *2012-13 Defence Annual Report* indicated that 0.6 per cent of members had a part-time leave without pay arrangement.[5] The 2014 AHRC audit report noted that data on the uptake of the five formal types of FWAs was both limited and unreliable, however, all three Services stated there was extensive use of informal FWAs but that these were not being reported.[6]

Although each of the Services has contended that FWAs are being used extensively, there is evidence to suggest that members' perceptions of and access to flexible work remain an issue. For example, the latest 'YourSay' Defence survey results, published in May 2013, indicated that only 63 per cent of women and 57 per cent of men believed their manager actively supported work-life balance or FWAs; furthermore, 41 per cent of women and 44 per cent of men believed that if they accessed FWAs their career progression would suffer.[7]

The study project

Background research

The term 'flexible work arrangements' is broad and can encompass a range of arrangements, including adjustments to the timing and location of work or the tasks undertaken (for example, flexitime, job sharing, part-time work, telework and personal leave); providing caregiving and health benefits (for example, child and elder care); and providing financial and information support for non-work roles (for example, vouchers and referral services).[8]

While studies have predominantly addressed more formal and longer-term forms of flexibility (for example, part-time work, work from home arrangements and parental leave), FWAs can also include short-term, occasional, *ad hoc* and informal arrangements (for example, flexible start and finish times, and carer's leave).

The increasing demand for FWAs and other work-life initiatives has been influenced by a range of social, economic and political factors including:

- changes in family structures, work systems and social roles;
- inter-generational differences in work values;
- an increasingly knowledgeable and expert workforce;
- greater numbers of dual-earner couples and sole parents;
- public support for childcare; and
- the rapid expansion of information technology allowing work portability.[9]

Flexible work policies support employees to integrate a range of work and non-work commitments. However, while caring responsibilities tend to dominate discussions of why workers seek flexibility, some employees also require flexibility in order to fulfil non-family obligations. Providing opportunities for flexible work is often seen by senior managers and human resources professionals as an integral part of a diverse, competitive and efficient organisation.[10]

However, there is consistent evidence across a range of organisations that even when these policies are well conceived and intended to assist employees, they do not always live up to their goals. Indeed, some have argued that despite providing formally-defined FWA provisions, the organisation of work around the 'ideal worker', unencumbered by family or other external obligations, has remained largely unchallenged.[11]

Central to concerns about the connections between organisational-level FWA initiatives and the everyday experiences of employees is the role of the supervisor who, due to their status and power as a decision-maker, can be highly influential by encouraging or discouraging employees' efforts to balance their work and personal lives.[12] In this way, supervisors are instrumental in the uptake of formal FWA initiatives, as well as in supporting informal arrangements that may not be enshrined in formal documentation.[13] Manager support, as a component of the broader climate of an organisation, is a key factor which moderates the link between the promotion of work-life integration policies and employees' use of such policies.[14]

In light of the emphasis in the ADF on the significance of FWA policies and practices as crucial strategies to achieve recruitment and retention goals and create an inclusive work culture, we examined the types of requests for FWAs made by personnel, and supervisor responses to these requests. Importantly, we focused on both formal requests (enshrined in current ADF policies and focused on in the AHRC reports) and informal, short-term and *ad hoc* requests.

Although informal requests are far less visible and are not captured in routine organisational data collection, they have a potentially profound effect on the ability of ADF members to manage their work and personal lives. Our examination of the extent to which supervisors support specific FWA requests provides an empirical snapshot that can be considered in light of broader concerns about supervisor support and career detriment raised in the 'YourSay' surveys. The study also yields insights into the types of requests that are considered more or less problematic in different Service environments.

Methods

Data comprised individual interviews by researchers from Queensland University of Technology with 130 Navy, Army and Air Force personnel. Site visits were arranged via commanding officers at 12 separate units in five Australian states. A range of units were represented, including combat support, training, maintenance and operational functions. In-depth, semi-structured interviews were conducted in a private meeting room at each base. After gaining individual consent from volunteer participants, all interviews were audio-recorded and later transcribed for analysis.

Initial interview questions asked if, in the previous 12 months, participants had sought adjustments to their work arrangements across four major flexible work categories: hours of work, work location, work tasks and time off. This article reports on the numbers of requests and responses to requests in these four thematic areas, including 18 distinct sub-types of FWAs.

Other interview questions, which were not the subject of analysis for this article, explored the reasons for requests, the process of negotiating requests, the nature of supervisory and organisational support for FWAs, reasons for not making requests (employee silence) and the formulation and communication of FWA policies in the ADF.

Sample

Of the 130 participants recruited to the study, five were at a high rank. Quantitative data was not collected for these participants as there was a risk they could be identified. The Service and gender profile of the remaining 125 participants is shown in Table 2. They were aged between 21 and 59 years (mean 36.65). The majority of participants were employed as permanent members (95%), four were active reservists (3%) and two were on continuous full-time service (2%). More than two-thirds of the sample (88 participants, 67%) had served for 10 years or more. Only five participants (4%) had served for less than three years.

Forty one participants (33%) were commissioned officers, 41 (33%) were non-commissioned officers and 43 (34%) were other ranks. Around three-quarters (74%) of participants supervised other personnel. Two-thirds (65%) were responsible for dependent children and 7 per cent of these were single-parents. One in five participants (19%) was part of a couple without children, while 16 per cent were single with no children. Of the 100 participants in a relationship, 78 per cent had a partner engaged in paid work and 28 per cent of these were employed by Defence.

Table 2: Participants by gender and service

Service	Male		Female		Total	
	n	**%**	**n**	**%**	**n**	**%**
Navy	29	33.3	20	46.5	49	39.2
Army	29	35.6	6	14.0	35	28.0
Air Force	25	31.0	16	39.5	41	32.8
TOTAL	**83**	**66.4%**	**42**	**33.6%**	**125**	

Analysis

Demographic data and data on the number of types of FWA requests were entered into a statistical software package for analysis. Further, textual data was examined by searching within each major flexible work request category in order to provide a detailed picture of how FWAs were sought by individuals and managed by supervisors.

The results

The mean number of requests for FWAs by individual participants in the previous year was 8.14. All participants had sought adjustments to their working arrangements in at least one key flexibility category. As shown in Table 3 (overleaf), the most common types of requests were associated with 'time off' (mean 2.46) and changes to 'hours of work' (1.41). While the frequency of requests was high across all Services, the highest mean number of requests overall were by Air Force personnel (8.59) and the lowest number by Army personnel (7.66).

Table 3: Total number of requests by flexibility category and gender

Type	Requested		Not requested		Mean number of requests made	
	n	%	n	%	Male	Female
Time off	116	92.8	9	7.2	2.45	2.46
Changes to work hours	98	78.4	27	21.6	1.16	1.90
Changes to work location	106	84.8	19	15.2	1.25	1.31
Changes to work duties	51	40.8	74	59.2	0.39	0.71

Overall, as shown in Table 4, non-commissioned officers and other ranks were more likely to request adjustments to their work arrangements than officers (mean of 8.59 and 8.21 respectively, compared to 7.61 for officers). In contrast to officers, non-commissioned officers and other ranks were more likely to request adjustments around 'time off', whereas officers were more likely to request adjustments relating to 'location of work' (particularly work from home arrangements).

Table 4: Mean number of requests by rank

Type	Total Mean	Mean for Officers	Mean for Non-Commissioned Officers	Mean for Other Ranks
Time off	2.46	2.10	2.79	2.49
Changes to work hours	1.41	1.20	1.71	1.33
Changes to work location	1.27	1.42	1.24	1.16
Changes to work duties	0.50	0.44	0.49	0.56

Outcomes of requests

More than three-quarters of all requests were fully granted (76%). Requests that were 'partly granted' or 'declined' were more likely to be related to posting location (40%), the timing of annual leave or holidays (15%) and changes to the amount of flexibility in working times (12%).

The mean number of fully-granted requests per respondent was 6.19. Navy personnel were most likely to have their requests for FWAs fully granted (79%), compared to 77 per cent for Army and 70 per cent for Air Force personnel.

Requests for change to hours of work

As Table 5 illustrates, the most common request was for changes to start/finish times, with 87.7 per cent of these fully granted. Other forms of flexibility that were frequently requested included moving from full-time to part-time service, and changes to the amount of flexibility in working times. Air Force personnel made the most requests for changes to work hours and Army personnel the fewest (see Figure 1 overleaf).

Table 5: Outcomes of requests for changes to work hours (all Services)

Requested change	Total requests		Request outcome							
			fully granted		partially granted		declined		outcome pending	
	n	%	n	%	n	%	n	%	n	%
Full-time to part-time	14	11.2	7	50.0	6	42.9	1	7.1	0	0.0
Part-time to full-time	6	4.8	4	66.7	2	33.3	0	0.0	0	0.0
Change to start/finish time	73	58.4	64	87.7	6	8.2	0	0.0	3	4.1
Working school terms	3	2.4	3	100.0	0	0.0	0	0.0	0	0.0
Changes to amount of flexibility	49	39.2	40	81.6	9	16.3	0	0.0	1	2.0
Increase or decrease in hours	15	12.0	11	73.3	2	13.3	1	6.7	1	6.7
Other changes	9	7.2	6	66.7	2	22.2	0	0.0	1	11.1

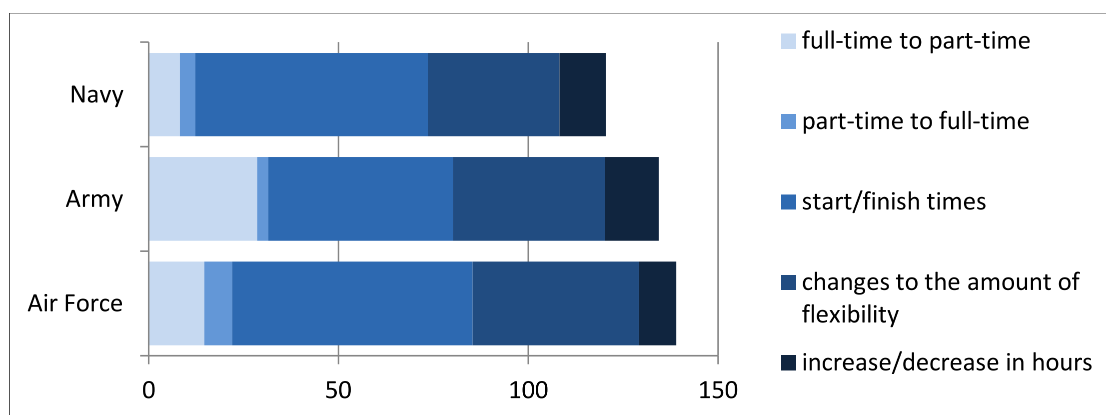


Figure 1: Requests for changes to work hours by Service (%)

Despite Air Force having the most requests for changes to work hours, Army personnel were the most likely to have their requests fully granted (84%), compared to 80 per cent for Air Force and 77 per cent for Navy. Across all three Services, officers had 90 per cent of their requests for changes to work hours fully granted, compared to 74 per cent for other ranks. Across all three Services, men had 85 per cent of their requests for changes to work hours fully granted, compared to 73 per cent of women.

Requests for time off

The most common leave request related to the timing of annual leave. The majority of these requests were fully (85.1%) or partially (9.6%) granted. Requests to access sick and carer's leave were also common; again, the vast majority of these requests were fully granted. Almost half of all participants (48%) had requested other forms of time-off including study leave, bereavement/compassionate leave, long service leave, time off in lieu, convalescence leave, short absence leave, travel leave, removals leave, war service leave, stress leave and ADF sport leave. As illustrated in Table 6, 90 per cent of these requests were fully granted.

Table 6: Outcomes of requests for time off (all Services)

Requested change	Total requests		Request outcome							
			fully granted		partially granted		declined		outcome pending	
	n	%	n	%	n	%	n	%	n	%
Timing of annual leave	94	75.2	80	85.1	9	9.6	5	5.3	0	0.0
Sick leave	61	48.8	56	91.8	5	8.2	0	0.0	0	0.0
Carer's leave	61	48.8	55	90.2	3	4.9	3	4.9	0	0.0
Timing of parental leave	31	24.8	28	90.3	3	9.7	0	0.0	0	0.0
Other leave	60	48.0	54	90.0	4	6.7	0	0.0	2	3.3

As shown in Figure 2, Air Force personnel made the most requests for time-off (95.1%) and Army the fewest (91.4%). Navy personnel were the most likely to have their request fully granted (92%), compared to 89 per cent for Air Force and 85 per cent for Army. Across all Services, men had 88 per cent of their requests for time-off fully granted, compared to 91 per cent of women.

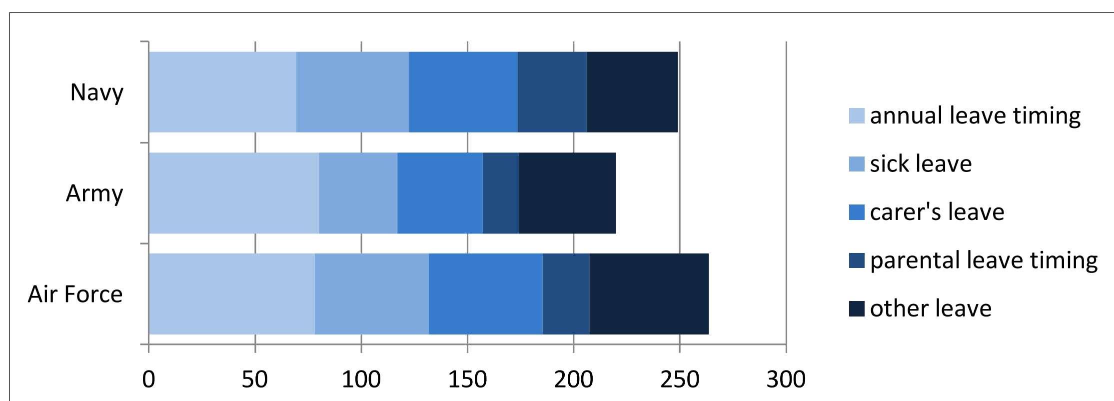


Figure 2: Requests for time off by Service (%)

Changes to Service duties

Across all Services, 23 per cent of participants had requested a change to their workload; two-thirds of these requests (65.5%) were fully granted (see Table 7). Over a quarter (26%) of personnel had requested a change to their duties in the last 12 months and 84.8 per cent of these requests were fully granted. Navy personnel were most likely to have their request for a change in duties fully granted (86%), compared to 75 per cent of Army and 59 per cent of Air Force personnel. Figure 3 depicts the requests for changes to work tasks by Service.

Table 7: Requests for changes to work tasks (all Services)

Requested change	Total requests		Request outcome							
			fully granted		partially granted		declined		outcome pending	
	n	%	n	%	n	%	n	%	n	%
Reduce/increase work load	29	23.2	19	65.5	5	17.2	4	13.8	1	3.4
Altered duties	33	26.4	28	84.8	2	6.1	2	6.1	1	3.0

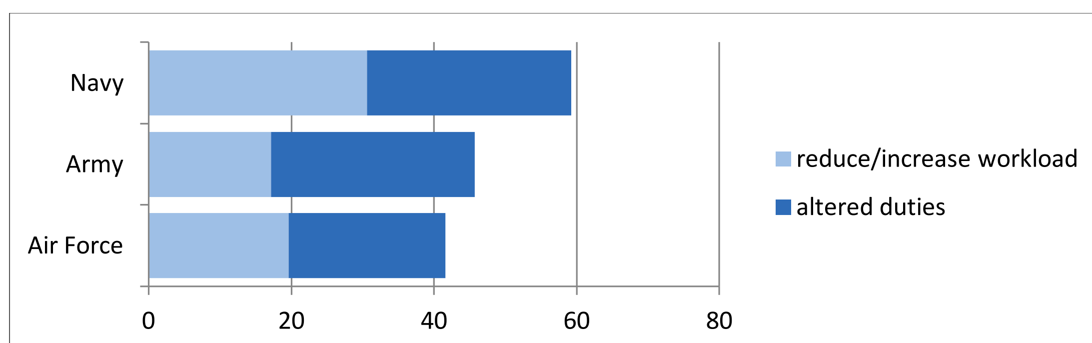


Figure 3: Requests for changes to work tasks by Service (%)

Changes to work location

Requests for changes to work location included changes to postings, working from home or from a remote site, and taking work home after-hours. Overall, 62 per cent of requests for changes in work location were fully granted. Army personnel were most likely to have their request fully granted (71%), compared to 66 per cent of Navy and 50 per cent of Air Force personnel.

The majority of requests for changes to work location were in relation to requests for postings. More than three-quarters (78.4%) of participants had made a specific posting request in the previous 12 months and 54.6 per cent of these requests were fully granted. Figure 4 (overleaf) depicts requests for changes to work location by Service.

Table 8: Requests for changes to work location, all Services

Requested change	Total requests		Request outcome							
			fully granted		partially granted		declined		outcome pending	
	n	%	n	%	n	%	n	%	n	%
Working from home	27	21.6	19	70.4	5	18.5	3	11.1	0	0
Taking work home after hours	23	18.4	21	91.3	1	4.3	1	4.31	0	0
Posting preference	98	78.4	53	54.6	31	32.0	8	8.2	5	5.2
Work from remote location	12	9.6	6	54.5	3	27.3	2	18.2	0	0

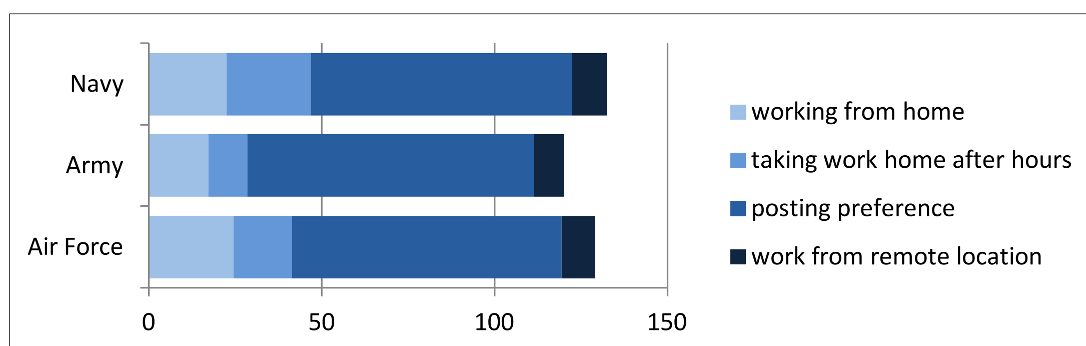


Figure 4: Requests for changes to work location by Service (%)

Debunking myths related to flexible work in the ADF

The analysis undertaken for this study suggests there are significant gaps between the popular understanding of flexible work in the ADF and the experience of service personnel.

Policy vs practice

Although the Service Chiefs have agreed on a target of 2 per cent for the use of FWAs by the end of 2014, a recent report on flexible work in the Army concluded that there was still considerable scope for greater participation.[15] In contrast to these relatively small and incremental aspirations for increasing the uptake of FWAs, our analysis demonstrates that they are already extensively used in the Services.

Indeed, the study provides strong evidence that FWAs go beyond a 'minority interest'. Rather, the majority of personnel seek FWAs, do so frequently and are successful in gaining approval for such adjustments. This was evidenced in the fact that participants had made, on average, around eight requests for flexibility in the previous 12 months across a wide variety of flexibility types, and that three-quarters of these requests had been granted.

However, very few of these requests aligned with existing, documented ADF policy as outlined in the introduction to this article. In contrast, many requests were occasional, short-term, one-off or *ad hoc* and, while some request categories may have been implicitly encompassed in the formal policy, they were rarely recorded as a formal FWA. Moreover, unless the agreement was for a period greater than four weeks, they were unlikely to be included in any official records.

Our analysis indicates that the majority of personnel were motivated to negotiate changes to their working hours to enable them to remain a full-time, permanent member. This included building flexibility into working times, accessing a range of leave entitlements and working from home or occasionally from a remote location.

Typical flexibility requests included adjustments such as starting work later and finishing later in order to drop children at day care, leaving early one day a week in order to participate in sport, or working from home for a set period during home renovations. Illustrating the informal nature of many requests was that they were often negotiated at the last minute and individually with supervisors; they did not involve paperwork and were not seen as a formal FWA by either the requestor or approver but rather as an individual accommodation as a reward for service.

The Defence Attitude Survey indicates that one of the principal reasons for leaving the Service is a 'lack of control over life'.[16] However, the ability to negotiate access to flexibility enables personnel to tailor their requests to their specific needs. For example, rather than entering into a formal 'variable working hours' agreement, they simply discuss what they need with their

supervisors, whether it be several weeks of flexible working in order to manage responsibilities during school holidays or an occasional early finish to attend a university lecture.

Furthermore, in contrast to the frequently voiced fear that FWAs are not compatible with operational requirements, our analysis suggests that members had a clear understanding of the potential impacts of their flexibility requests on the workload of co-workers and, as a consequence, generally only made requests if they believed their unit would experience minimal disruptions.

It has been suggested that it is not the FWAs policy that is problematic in the ADF but rather the way it has been implemented.[17] The formal policy is a critical means of ensuring that personnel can balance service with other responsibilities, particularly at important junctures in their lives, such as around the birth of a child, during a major health event or when a partner is posted overseas.

However, access to informal FWAs is also of vital importance, enabling members to manage their work and non-work obligations by making minor adjustments to their work arrangements. The current emphasis in the ADF on revising and codifying policy and reporting mechanisms may be directing attention away from the informal, occasional and more individually-tailored FWAs that our analysis suggests are widely embedded in everyday working practices across the Services and which are deeply valued by personnel.

Who are the beneficiaries?

Women make up 13.8 per cent of ADF personnel[18] and, as noted in the introduction, the drivers for creating access to FWAs in the ADF are part of a strategy to increase the number of women serving and build a culture of inclusivity and equity. The link between gender equality and FWAs was made explicitly by the AHRC in its review into the treatment of women in the ADF.

Recently, this was reiterated by the Chief of Army when he described how he had established an Army Diversity Council to set policy initiatives relevant to women and other disadvantaged groups with regard to recruitment, retention, training and flexible work practices. The General noted that 'generally speaking, great policy for women is great policy for everyone'.[19]

This agenda, and the rhetoric around FWAs in the community more broadly and in the ADF specifically, assumes that FWAs will benefit women rather than men and that it is mothers, in particular, who will seek to use FWAs. In contrast, our analysis shows that both men and women make extensive use of FWAs in the ADF. Similar proportions of men and women made requests for changes to hours of work (78.3% and 78.6% respectively) and a higher proportion of men requested changes to work location than women (86.7% and 81% respectively).

Furthermore, men were more likely to have their requests fully granted (78%) than women (73%) in three of the four flexibility categories explored: changes to work hours, changes to duties and requests to change the location of work. The only area where women were more likely than men to have their request fully granted was when that request related to time-off (91% compared to 88%).

The ADF has pursued a policy aimed at strengthening individual members' commitment by providing support mechanisms for service families.[20] For example, the 'Army Work-Life Balance Strategy' explicitly aims to help members maintain a balance between paid work and personal, community and cultural responsibilities, interests and obligations.[21]

Our analysis points to a growing acceptance by service personnel that FWAs are compatible with a service career, and that men as well as women can access and benefit from flexibility relating to the location of their work, their hours of work, their roles and duties, and leave entitlements. FWAs in the ADF should no longer be seen as a threat to capability, as 'women's business', or even intended solely for the benefit of personnel who are parents. Instead, they are widely used and valued by the vast majority of personnel—irrespective of gender or the nature of obligations in their personal spheres.

Conclusion

We have asserted through the findings of this study that it is a myth that FWAs in the ADF are a minority interest, dominated by requests for part-time work and that they are used exclusively by women. Rather, our analysis shows that FWAs are used extensively by personnel in the ADF; the average member making more than eight requests for flexibility in a 12-month period, with the majority of these being fully granted.

Furthermore, access to FWAs—while continuing to be associated predominantly with women's needs in broader rhetoric and policy—are, in everyday work settings, requested by both men and women and approved in high proportion for both sexes. Thus, this research points to a key policy-practice gap in highlighting the importance of informal, occasional and *ad hoc* access to flexibility to members, despite a policy-level framework focused on formal, long-term and planned forms of flexibility. Informal flexibility enables servicemen and -women to combine serving with the messy, everyday challenges that are part of modern-day life.

We argue that the ADF needs to adopt a broader understanding of what flexibility is and can be, including flexibility relating to hours of work, time-off, changes to duties and location of work. Many of these forms of FWAs are already used and valued by members; however, there is a significant risk that the growing pressure on the ADF to deliver results relating to its formal policy may close down access to informal mechanisms and add layers of bureaucracy which will impact on how supervisors respond to requests.

The ADF is challenged with transforming itself to better represent the society in which it operates, while continuing to meet its operational needs.[22] Recognising the importance of informal and formal access to FWAs for both servicemen and -women is likely to further the reputational and operational advantages of the ADF in driving culture change, promoting inclusion and enabling personnel to effectively integrate serving in the Navy, Army and Air Force with commitments in their personal lives.

Dr Abby Cathcart is an Associate Professor of Management at Queensland University of Technology (QUT). Her publications include research on social responsibility, governance, flexible work and employee voice and silence. She is currently working on an Australian Research Council project exploring customised work practices in a wide range of organisations, including small not-for-profits, a large finance company and the ADF.

Paula McDonald is professor of employment relations and ARC Future Research Fellow in the QUT Business School. Her research on flexible work policy and practice spans 15 years and a wide range of industry sectors including finance, higher education, local and state government, not-for-profits and, most recently, Defence. She has published an international edited collection, three book chapters and 12 journal articles on the topic.

Dr Deanna Grant-Smith is a postdoctoral research fellow in the QUT Business School. Informed by her extensive experience working in government, Dr Grant-Smith's research focuses on a range of contemporary policy and public sector management issues including sustainability, stakeholder engagement and collaborative governance, gendered access to services, and early career professional employment.

ACKNOWLEDGEMENTS AND DISCLAIMER

This research was undertaken with the support of an Australian Research Council Discovery Grant (DP 120101560) and additional funding from the ADF. Ethical approval of the study was received from the Australian Defence Human Research Ethics Committee and Queensland University of Technology Research Ethics Unit. The opinions expressed are those of the authors and do not necessarily reflect those of Defence or any extant policy.

NOTES

1. E. Broderick (ed.), *Australian Human Rights Commission (2012) Review into the treatment of women in the Australian Defence Force: Phase 2 Report,* The Australian Human Rights Commission: Sydney, 2012; E. Broderick (ed.), *Review into the treatment of women at the Australian Defence Force Academy: Audit Report,* Australian Human Rights Commission: Sydney, 2013.

2. Department of Defence, *Military Personnel Policy Manual*, Department of Defence: Canberra, 2013.

3. See, for example, L. Smallacombe, 'People Plan', *Navy News,* Vol. 56, No. 23, 5 December 2013, pp. 16-7, available at <www.defence.gov.au/news/navynews/editions/5623/5623.pdf> accessed 10 October 2014.

4. E. Broderick (ed.), *Review into the treatment of women in the Australian Defence Force: Audit Report,* The Australian Human Rights Commission: Sydney, 2014.

5. Department of Defence, *Department of Defence Census 2011 Public Report,* Australian Government: Canberra, 2012; Department of Defence, *Defence Annual Report: 2012-13: Supplementary Content - Women in the ADF,* Australian Government Department of Defence: Canberra, 2013.

6. Broderick, *Review into the treatment of women in the Australian Defence Force,* p. 128.

7. As reported in Department of Defence, *Defence Annual Report: 2012-13: Supplementary Content - Women in the ADF*.

8. A. McCarthy, C. Darcy and G. Grady, 'Work-life balance policy and practice: understanding line manager attitudes and behaviours', *Human Resource Management Review*, Vol. 20, 2010, pp. 158-67; A. Ryan and E. Ernst Kossek, 'Work-life policy implementation: breaking down or creating barriers to inclusiveness', *Human Resource Management*, Vol. 47, 2008, pp. 295-310.

9. M. Pitt-Catsouphes and K. Christensen, 'Unmasking the taken for granted', *Community, Work & Family*, Vol. 7, Issue 2, 2004, pp. 123-42; J.H. Greenhaus and G.N. Powell, 'When work and family collide: deciding between competing role demands', *Organizational Behavior and Human Decision Processes*, Vol. 90, 2003, pp. 291-303; S. Fleetwood, 'Why work-life balance now?', *International Journal of Human Resource Management,* Vol. 18, 2007, pp. 387-400.

10. E. Michielsens, C. Bingham and L. Clarke, 'Managing diversity through flexible work arrangements: management perspectives', *Employee Relations,* Vol. 36, 2014, pp. 49-69.

11. P. McDonald, K. Townsend and A. Wharton, 'The legitimation and reproduction of discourse-practice gaps in work-life balance', *Personnel Review,* Vol. 42, 2013, pp. 205-22; S. Charlesworth and M. Baird, 'Getting gender on the agenda: the tale of two organisations', *Women in Management Review*, Vol. 22, 2007, pp. 391-404.

12. C. Straub, 'Antecedents and organizational consequences of family supportive supervisor behaviour: a multilevel conceptual framework for research', *Human Resource Management Review*, Vol. 22, 2012, pp. 15-26; C.A. Thompson, C.C Thomas and M. Maier, 'Work-family conflict and the bottom line: reassessing corporate policies and initiatives', in U. Sekaran and F. T. Leong (eds.), *Woman-Power: managing in times of demographic turbulence*, Sage Publications: Newbury Park, 1992, pp. 59-84.

13. E. Knies, 'When do supervisors support 'tailor-made' work arrangements? An exploratory study', *Labour and Industry*, Vol. 21, 2011, pp. 621-43.

14. S. Hornung, D. Rousseau, and J. Glaser, 'Creating flexible work arrangements through idiosyncratic deals', *Journal of Applied Psychology*, Vol. 93, 2008, pp. 655-64; P. McDonald, L. Bradley and K Brown, 'Visibility in the workplace: still an ingredient for career success', *International Journal of Human Resource Management*, Vol. 19, 2008, pp. 2198-215.

15. K. Skinner and C. Diggins, 'Organisational Culture: family friendly Army - first class policy, second class implementation', *Australian Army Journal,* Vol. X, 2013, pp. 173-87.

16. K. Thomas and S. Bell, 'Competing for the Best and Brightest: recruitment and retention in the Australian Defence Force', *Security Challenges,* Vol. 3, 2007, pp. 97-114.

17. Skinner and Diggins, 'Organisational Culture'.

18. Australian Bureau of Statistics, *ABS Year Book 2012,* Australian Bureau of Statistics: Canberra, 2012.

19. F. Krautil, 'A problem admitted is the first step: an interview with Lieutenant General David Morrison', *HRmonthly*, March 2014, pp.17-9.

20 J. Armstrong, *Defence Families. Defence Life,* Strike Publications: Ipswich, 2013; Air Force News, 'Free health care for families', *Air Force News: The official newspaper of the Royal Australian Air Force,* Directorate of Defence News: Canberra, 2014, p. 22.

21 A.A John, 'Organisational Culture: from institution to occupation: Australian Army culture in transition', *Australian Army Journal,* Vol. X, 2013, pp. 187-201.

22 C. Corbett, 'Our Navy Blues: the RAN's struggle to win hearts and minds', *The Monthly*, April 2014, pp. 16-20, available at <http://www.themonthly.com.au/issue/2014/march/1396270800/claire-corbett/royal-australian-navys-struggle-our-hearts-and-minds> accessed 12 October 2014.

East by South-West: the relevance and opportunities for the Australia-Canada security relationship [1]

Captain Michele Miller, RAN

> If you took the United States away from Canada's southern border, if you took away the French influence, then Australia and Canada are very, very comparable: large land mass countries, federated states with a lot of geographic, social and economic diversity from the west coast to the east coast.
>
> Australia's Minister for Defence in 2011[2]

Introduction

As part of the Australian Government's preparation for the 2015 Defence White Paper, it released a *Defence Issues Paper* in May 2014 that poses strategic questions about Australia's future defence policy settings and capability plans.[3] One issue for strategic assessment is Australia's traditional security ties and whether there are opportunities to strengthen cooperation. Specifically, the paper asks if Australia's longstanding defence relationship with Canada, among others, is still relevant and whether Australia should consider options to increase cooperation on defence industry development.[4]

Linked to this is a key question as to how the ADF can use such relationships and cooperation to promote regional stability and advance Australia's national interests and influence.[5] However, there is a challenge for Canada and Australia: the relationship is described by the Australian Prime Minister as 'strong but under-developed even though we are as like-minded as any two countries can be'.[6] Clearly there is focus needed to improve engagement, with security and defence cooperation being two key areas.

This article will argue that Australia's security relationship with Canada remains relevant and that there are new opportunities for closer bilateral military engagement. It will first examine why the security relationship is important and relevant, especially in terms of regional security risks and shared national interests. It will then examine options for closer defence cooperation in two ways; first, in direct arrangements, notably in capability development; then in coordinated military engagement to strengthen regional security and build military capacity. The article will conclude by identifying the challenge to governments to improve cooperation, namely in relation to time and resources.

Why the relationship is relevant

At the end of 2014, a close but low-key diplomatic relationship between Australia and Canada will have existed for 75 years, although the trade relationship extends back 100 years and the military relationship started in the Boer War. Despite the great distance between the countries, as shown in Figure 1, Canada and Australia are significant investors in each other's markets and there are numerous existing bilateral agreements, with more instigated each year particularly in resource-based sectors.[7]

However, despite many of the same national interests in the Asia-Pacific area, cooperation on regional matters has been *ad hoc*—both Australia and Canada are present in many of the same multilateral forums but collaboration on issues of common concern is inconsistent.[8]

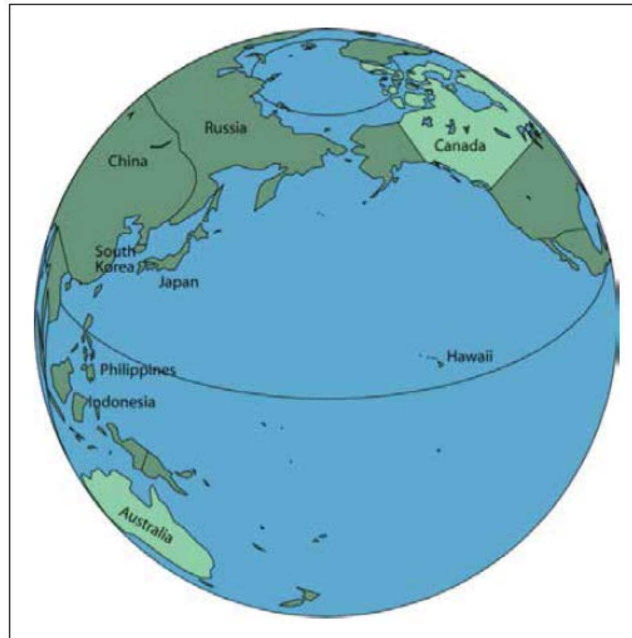


Figure 1: Australia and Canada in the Asia-Pacific region[9]

As economic power moves from the West to the East, and as China rises and challenges the US for strategic power in the region, the instability caused by longstanding territorial disputes and a lack of trust means that security cooperation is growing in importance.[10] Specifically, it is in the interests of both Canada and Australia—as mid-sized economies deeply dependent on trade with Asia—to foster a rules-based regional order and maintain regional peace and security.[11] As noted in a February 2014 report by Leonard Edwards and Peter Jennings addressing the role of Canada and Australia in East Asia:

> Economic and security cooperation go hand in hand. Economic integration can leaven tensions; security cooperation and institutional face-time can build trade ties by maintaining stability, reducing mistrust and preventing potentially costly escalation of regional disputes.[12]

However, the Asia-Pacific security order is built on a system of unilateral preparedness, a US-centred bilateral alliance system, and sometimes ineffectual regional institutions that prefer consensus building over negotiation and rules.[13] By necessity, Australia is deeply engaged in this system to bolster regional governance mechanisms and strengthen regional security. However, since 1997, Canada's commitment in the Asia-Pacific has waned and its decision at that time to cease several engagement programs caused strategic reputational damage, especially with ASEAN members.[14]

Many Canadian security commentators have argued that Canada needs sustained engagement before it would be welcomed back into the emerging regional architecture.[15] Canada's dilemma is that its primary economic and security partner is the US, whereas its prosperity is increasingly linked more closely to the vitality of Asia's economy and the stability of the Asia-Pacific.[16] Additionally, fiscal pressures mean that any increase in engagement will need to be offset in other areas.

Nevertheless, it is evident that the Canadian Government has decided to leverage its longstanding military engagement activities in the region as a practical means to convey its commitment.[17] Consequently, the opportunity exists for increasing Australia-Canada bilateral military cooperation to enhance the national security interests of both Canada and Australia. An improved bilateral relationship is important for both what it can bring to serve the interests of each country but also how it can influence regional peace and stability.

For Australia, the engagement of Canada at a regional level means that there is an additional like-minded interlocutor at economic and security forums, as well as another capable military it can cooperate with in multilateral defence diplomacy, including the US. Additionally, as Australia is keen to develop its relationship with NATO to a strategic partnership, Canada can offer its knowledge and experience as an important NATO member.[18]

For Canada, the benefits are similar but there is an added benefit of having a 'strategic cousin' that could assist Canada to sustain a credible level of focus on the region and achieve its strategic aspirations.[19] The challenge then, particularly in a common resource-constrained environment, is how to leverage this relationship more efficiently and effectively.

Strengthening defence cooperation

Canada's defence relationship with Australia is its largest in the Asia-Pacific after the US, and while there are over 300 annual visits (primarily related to science and technology, and intelligence), training exchanges and defence meetings between the countries, there are no bilateral agreements that bind the two to cooperate.[20] Indeed, formal bilateral strategic dialogue at ministerial-, Chief of Defence Force- and Deputy Secretary-level only commenced in March 2012.

For both countries, their most important defence relationship is with the US. Most Canada-Australia engagement is in some way linked with the US through the various tactical and technical five-nation multilateral programs and forums.[21] Importantly, it is the 'Five Eyes' intelligence community, in which both Canada and Australia make significant contributions, that the Australian Government sees as strategically vital as it 'still forms the bedrock of our capacity to understand strategic developments in the Indo-Pacific and beyond'.[22]

However, within the existing five-nation forums, fostering closer Australia-Canada bilateral cooperation could begin with a joint assessment of present personnel exchanges and cooperative frameworks to avoid duplication and gauge whether they meet future needs. Where efficiencies are made, both the intellectual effort and personnel resources should then be reinvested into newer areas of cooperation, such as capability development and acquisition.

In 2008, Canada articulated in *Canada First Defence Strategy* its plans to replace its major capabilities.[23] Since then, however, fiscal constraint has resulted in operating budgets being dramatically cut and significant delays in acquisition projects, partially as a result of the retrenchment of experienced acquisition personnel.[24] In this light, the Australian and Canadian Defence Ministers in 2011 established a strategic dialogue on defence reform, capability, procurement and budget management to discuss experiences and common challenges.[25] In 2014, with both countries again facing federal deficits and constrained defence budgets, it should be a high priority to pursue cooperative dividends in these areas.[26]

There have been suggestions that to achieve economies of scale and effort, Australia could build submarines for Canada, and Canada could build offshore patrol vessels for Australia to use in the Southern Ocean. However, these programs are arguably too well advanced for this to be realistic—the focus needs to be on plans that will deliver in 20-30 years so that cooperative savings can be built in early, including with industry.[27]

An opportunity for today is the sharing of capability development experience and processes. Specifically, there could be cooperation in needs analysis, requirements analysis, risk analysis and perhaps tender evaluation and through-life modelling, perhaps with one country the 'red team' for the other. Additionally, there could be a valuable sharing of lessons learned from contemporary major acquisitions. While needing to be cognisant of the strategic and economic relationships with the US that both constrain and support defence cooperation, Canada and Australia could nonetheless also campaign together to be a louder voice in the US defence trade, sustainment and modernisation systems.[28] This could work for aircraft such as the C-130J and C-17 (and potentially the F-35 in the future), which all three countries operate.

In terms of future indigenous build programs, a recent report identified 'a number of areas where Canada and Australia could develop cooperative activities in the future that would benefit both nations and provide some scale of production'.[29] Significantly, the use of 'could' is highly dependent on the respective Government's decisions on matters of national interest (such as jobs generation through shipbuilding) and early industry agreement. However, initiatives that integrate defence industry markets and provide opportunities for industry to reduce costs and be more competitive are worth pursuing.

Key long-term areas could be in cyber security, electronic warfare and simulation, where compatible capabilities may provide opportunities to supply US and NATO forces as well. This could be further leveraged through many of the Canadian and Australian defence contractors which have US parent companies.[30] The important issue is to have the respective Governments agree to deep-level procurement integration, taking into account the attendant political risks, and then decide early to cooperate and inform industry. In this way, the relationship between Australian and Canadian defence industries would more effectively form part of the broader defence relationship.[31]

Strengthening military cooperation in the Asia-Pacific region

At the 2013 Shangri-La Dialogue in Singapore, Canada's Minister for National Defence made a concerted pitch to the Asia-Pacific nations to assure them that Canada recognised its past engagement shortfalls and emphasised its recommitment to the region, specifically through military cooperation.[32]

Canada would reasonably have an expectation that Australia will assist it to join the ASEAN's 'Defence Ministers Meeting Plus' and the East Asia Summit when membership is reopened. However, Australia also faces a need to ensure its own voice is heard in Southeast Asia, which may mean that 'Canberra isn't disposed to support Ottawa's membership bids'.[33]

Nevertheless, there are already multiple multilateral security cooperation mechanisms operating in the region, as shown in Figure 2, often with overlapping responsibilities. Hence, the best form of cooperation 'might well be separate from each other, drawing on the different strengths of each country, but in ways that project a common message'.[34]

Australia and Canada should collaborate on improving the effectiveness *within* these organisations, as well as sharing the effort needed to engage effectively *with* these organisations.[35] For instance, Canada and Australia should push to align working group agendas, for example on maritime security, between the ASEAN Regional Forum and the ASEAN Defence Ministers Meeting Plus.[36]

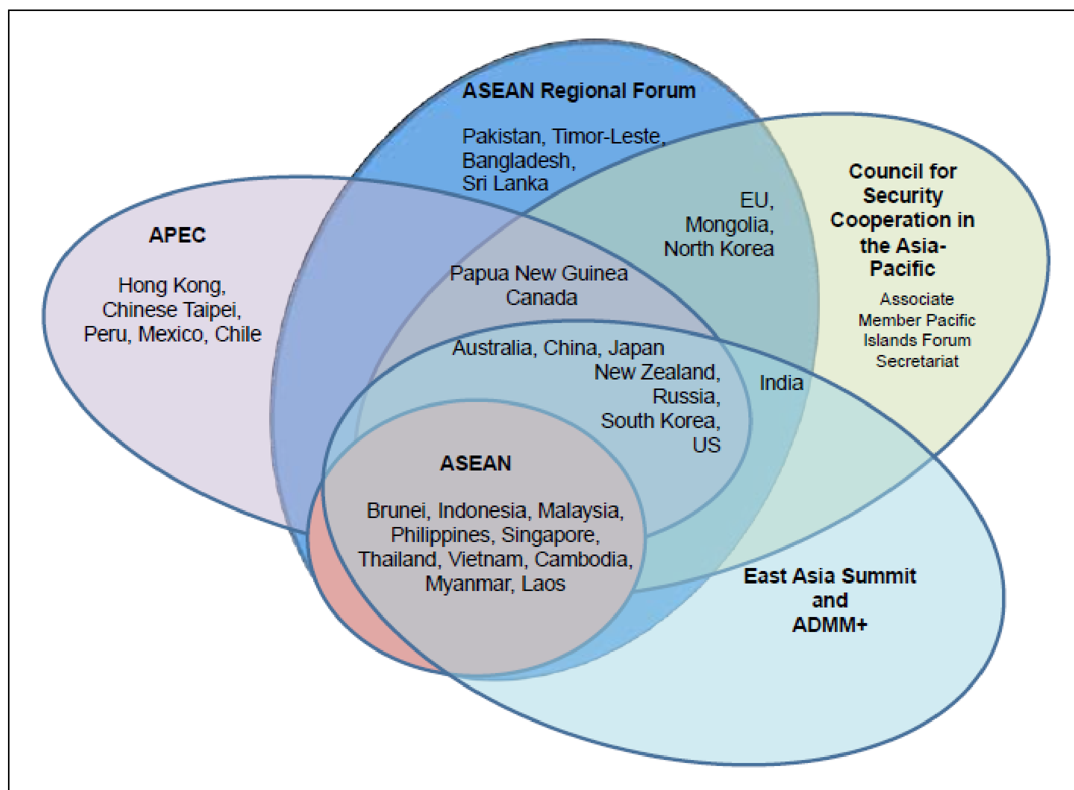


Figure 2: The Asia-Pacific's regional security architecture[37]

At a practical level, Canada and Australia continue to progress military capacity-building activities with regional partners in peacekeeping operations training, strengthening counter-terrorism collaboration, enhancing maritime security cooperation, and sharing lessons and training on humanitarian assistance and disaster relief. The key bilateral cooperation aspect is to ensure there is no duplication and that lessons learned on regional defence engagement are shared to improve efforts. Canada and Australia should develop formal, regular ways to align these engagements.

Australia and Canada could also seek opportunities together to enhance multilateral defence cooperation. As articulated by Sarah Norgrove, both countries 'bring sophisticated expertise and equipment to bear, and go far in socializing international norms and reciprocity into defence exercises in which they take part'.[38]

Maritime exercises are ideal activities, as participants can build trust 'but also engage with regional challenges and, in doing so, integrate into the region's strategic and security architecture'.[39] Building on the People's Liberation Army-Navy (PLA-N) engagement at the Rim of the Pacific Exercise in 2014 and previous RAN and PLA-N maritime exercises, Australia and Canada should work to develop common standards and protocols on interaction with China for basic exercises, search and rescue, manoeuvre drills and safe naval gunnery.

These protocols should extend to the China Coast Guard to encourage rules-based understanding and limit the escalation of maritime territorial disputes.[40] An additional benefit is that, as allies of the US, Australia and Canada can indirectly improve China-US engagement in ways that may be politically unacceptable between those two nations directly. Ultimately, such practical activities will make an important contribution to Canada's credible presence in the Asia-Pacific region and thus support its longer-term strategic security interests, as well as being an efficient and effective use of both Australian and Canadian defence cooperation capabilities.[41]

Conclusion

As the *Defence Issues Paper* states, '[as] an outward looking nation, Australia has long supported alliances and other relationships with like-minded countries as a way of promoting our security and making a contribution to regional and global security'.[42] By this measure, as this article has argued, the Canada-Australia security relationship is relevant particularly given the national interest of both countries in maintaining peace and stability in the Asia-Pacific region.

However, such relationships require resources and effort to build and sustain them. To improve bilateral security cooperation between Canada and Australia in the ways explored in this article, 'both governments will have to get serious about funding activities that bring the two militaries together, but the real commitments will be of time and intellectual energy'.[43] Perhaps for Australia it is as simple as the following statement from Prime Minister Tony Abbott in February 2014: 'Australians and Canadians should be more conscious not only of all that we have in common but of all the good that we might do together'.[44]

Captain Michele Miller graduated from ADFA in 1990 with a Bachelor of Science, majoring in Oceanography and Information Systems. She completed an additional year of study to gain an honours degree in Information Systems. As a maritime warfare officer, her early postings included service in the frigate HMAS Newcastle as gunnery officer, Commanding Officer of the patrol boat HMAS Bunbury, Operations Officer to Commodore Flotillas as a part of the Fleet Warfare Staff, and Executive Officer of the frigate HMAS Stuart, which included security operations in Iraqi territorial waters.

After attendance at the Australian Command and Staff Course and completion of a Graduate Diploma of Management in Defence Studies and a Graduate Certificate in Maritime Studies, she was posted to the Capability Development Group, before assuming command of the frigate HMAS Perth in 2007-08 and then Commander of the Sea Training Group. Her recent appointments have included Director of Sailors' Career Management, Director of the Navy People Career Management Agency, and Chief of Staff in Navy Strategic Command. She is currently attending the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College.

NOTES

1 This is an edited version of a paper developed by the author while attending the Defence and Strategic Studies Course at the Centre for Defence and Strategic Studies at the Australian Defence College in 2014.

2 Office of the [Australian] Minister for Defence, 'Press conference with Canada's Minister of National Defence Peter Mackay and Minister for Defence Stephen Smith', transcript, 12 September 2011, available at <http://www.minister.defence.gov.au/tag/smith-2/#main> accessed 22 August 2014.

3 Department of Defence, *Defence Issues Paper 2014,* Australian Government: Canberra, May 2014, available at <http://www.defence.gov.au/whitepaper/docs/defenceissuespaper2014.pdf> accessed 15 October 2014.

4 Department of Defence, *Defence Issues Paper 2014*, p. 17.

5 Department of Defence, *Defence Issues Paper 2014,* pp. 9 and 17.

6 Tony Abbott, 'Address to the Australia-Canada Economic Leadership Forum', Melbourne, 24 February 2014, available at <http://www.liberal.org.au/latest-news/2014/02/24/prime-minister-address-australia-canada-economic-leadership-forum> accessed 14 August 2014.

7 In 2013, total trade between the countries was A$3.383 billion, making this Australia's 22nd largest trading partner. Significantly, Australian investment in Canada was valued at A$53.7 billion in 2013, with over 80 Australian companies operating in Canada. Canadian investment in Australia was valued at A$26.9 billion in 2013, mostly in resources and manufacturing, but Canadian companies also own 27 per cent of the Port of Brisbane. See, for example, Department of Foreign Affairs and Trade (DFAT), *Canada Country Brief,* DFAT website, available at <https://www.dfat.gov.au/geo/canada/brief.html> accessed 22 July 2014.

8 Canada and Australia are both part of the G20, ASEAN Regional Forum, Asia-Pacific Economic Cooperation, the World Trade Organisation, the Cairns Group and the UN. In the UN, Australia, Canada and New Zealand operate in an informal arrangement known as the CANZ grouping: see DFAT, *Canada Country Brief.*

9 John Blaxland, *Strategic Cousins: Australian and Canadian expeditionary forces and the British and American Empires,* McGill-Queen's University Press: Montreal, 2006, p. xxxii.

10 Craig Stone, 'Canadian-Australian Opportunities for Defence Procurement and Industry Cooperation', Centre for International Governance Innovation (CIGI) Papers No. 22, CIGI, Ontario, January 2014, p. 5; Department of Defence, *Defence White Paper 2013,* Australian Government: Canberra, 2013, p. 67.

11 Three of Canada's top six export destinations are in Northeast Asia, and the ASEAN economies are Canada's seventh largest trading partner. For Australia, 37 per cent of total trade is with Northeast Asian economies (China, Japan and the Republic of Korea).

12 Leonard Edwards and Peter Jennings, *Facing West, Facing North: Canada and Australia in East Asia Special Report,* CIGI and the Australian Strategic Policy Institute (ASPI): Ontario and Canberra, February 2014, p. 10, available at <https://www.aspi.org.au/publications/facing-west,-facing-north-canada-and-australia-in-east-asia> accessed 16 October 2014.

13 National Conversation on Asia Task Force, *Securing Canada's Place in Asia: means, institutions and mechanisms,* Asia Pacific Foundation of Canada: Vancouver, August 2012, p. 21, available at <http://www.asiapacific.ca/research-report/securing-canadas-place-asia-means-institutions-and-mechanism> accessed 5 August 2014.

14 In 1997, the Canadian Government cancelled funding for the South China Sea dialogues, which had operated for five years promoting soft-power options to dispute management between claimants. According to the previous ASEAN Secretary-General, Surin Pitsuwan, Canada still has some ground to make up in the region to regain its reputation: see James Manicom, 'Canada's Return to East Asia: re-engagement through maritime diplomacy', Policy Brief No. 25, CIGI: Ontario, February 2013, p. 2.

15 Hugh Stephens, 'Canada and the EAS: when showing up is not enough', The Diplomat website, 27 September 2014, available at <http://thediplomat.com/2012/09/canada-and-the-eas-when-showing-up-is-not-enough/> accessed 5 August 2014.

16 National Conversation on Asia Task Force, *Securing Canada's Place in Asia,* p. 19; Canadian Armed Forces, *Canada's Defence Relations in the Asia-Pacific Region*, Government of Canada: Ottawa, 22 November 2013, available at <http://www.forces.gc.ca/en/news/article.page?doc=canada-s-defence-relations-in-the-asia-pacific-region/hob7h9ya> accessed 5 August 2014.

17 Manicom, 'Canada's Return to East Asia', p. 2.

18 Office of the [Australian] Minister for Defence, 'Press conference with Canada's Minister of National Defence Peter Mackay and Minister for Defence Stephen Smith'.

19 The term 'strategic cousins' was first used by John Blaxland in his *Australian Army Journal* article in 2003 to refer to the similarities between the military forces of Canada and Australia: John Blaxland, 'Strategic Cousins: Australian and Canadian military outlooks compared', *Australian Army Journal*, Vol. 1, No. 2, December 2003, pp. 139-46. It was then used by Canadian Prime Minister Stephen Harper when he addressed the Australian Parliament on 11 September 2007 to refer to shared national ideals.

20 Government of Canada, *Canada-Australia Defence Relations,* Government of Canada: Ottawa, 4 November 2013, available at < http://www.canadainternational.gc.ca/australia-australie/bilateral_relations_bilaterales/defence-defense.aspx?lang=eng> accessed 22 July 2014.

21 Currently shared five-nation military forums include The Technical Cooperation Program for defence scientific and information exchange; American, British, Canadian, Australian and New Zealand Armies' Program; Australia, Canada, New Zealand, United Kingdom and United States maritime information warfare interoperability forum; and the Air and Space Interoperability

Council. Australia and Canada also both participate annually in US Pacific Command's Chiefs of Defense Conference.

22 Department of Defence, *Defence Issues Paper 2014,* p. 17.

23 Prime Minister Stephen Harper, 'Canada First Defence Strategy', media release, 12 May 2008, available at <http://pm.gc.ca/eng/news/2008/05/12/canada-first-defence-strategy> accessed 16 October 2014.

24 Dave Perry, 'The Growing Gap between Defence Ends and Means: the disconnect between the *Canada First Defence Strategy* and the current defence budget', Vimy Paper No. 19, The Conference of Defence Associations Institute: Ottawa, June 2014, pp. 1 and 7, available at <http://www.cdainstitute.ca/images/PerryBudgetJune2014.pdf> accessed 21 August 2014.

25 Office of the [Australian] Minister for Defence, 'Press conference with Canada's Minister of National Defence Peter Mackay and Minister for Defence Stephen Smith'.

26 For a good discussion on this issue, see Craig Stone's two publications 'Canadian-Australian Opportunities for Defence Procurement and Industry Cooperation' and *Prioritizing Defence Industry Capabilities: lessons for Canada from Australia*, Canadian Defence & Foreign Affairs Institute: Calgary, 2014.

27 Edwards and Jennings, *Facing West, Facing North,* p. 14.

28 Stone, 'Canadian-Australian Opportunities for Defence Procurement and Industry Cooperation', p. 7.

29 Stone, 'Canadian-Australian Opportunities for Defence Procurement and Industry Cooperation', p. 12.

30 For instance, Lockheed Martin, Boeing, General Dynamics Land Systems, Thales, Raytheon and Sikorsky originate in either the US or Europe.

31 Department of Defence, *Defence White Paper 2013*, p. 55.

32 Peter MacKay, 'New Trends in Asia-Pacific Security', Address by the Minister of National Defence Canada, Fourth Plenary Session Shangri-La Dialogue 2013, Singapore, 2 June 2013, available at <https://www.iiss.org/en/events/shangri%20la%20dialogue/archive/shangri-la-dialogue-2013-c890/fourth-plenary-session-0f17/mackay-1f8b> accessed 14 August 2014.

33 Peter Jennings, 'Australia and Canada: a tale of two Tories', The Strategist website, ASPI, 23 May 2014, available at <http://www.aspistrategist.org.au/australia-and-canada-a-tale-of-two-tories/> accessed 14 August 2014.

34 Peter Jennings and Len Edwards, 'Proceedings and Outcomes Statement', Workshop on Promoting Closer Defence and Security Cooperation in the Asia-Pacific, ASPI and CIGI, Singapore, 2 June 2013, p. 6, available at < http://www.cigionline.org/sites/default/files/CIGI-ASPI%20Shangri-La%20Workshop%20Report.pdf> accessed 6 August 2014.

35 Canada and Australia are both presently part of the following security organisations that operate in the Asia-Pacific: ASEAN Regional Forum; Western Pacific Naval Symposium; Proliferation Security Initiative; the Shangri-La dialogue; Exercise RIMPAC; Asia-Pacific Economic Cooperation; and Council for Security Cooperation in the Asia-Pacific, which is a Track 2 dialogue that informs the ARF.

36 Edwards and Jennings, *Facing West, Facing North,* p. 13.

37 Sourced from Edwards and Jennings, *Facing West, Facing North,* p. 10.

38 Sarah Norgrove, 'Transnational Challenges and Future Security Cooperation: the Australia-Canada relationship', Australia-Canada Security Cooperation in the Asia-Pacific Paper No. 2, ASPI and CIGI: Canberra and Ontario, September 2013, p. 11.

39 Norgrove, 'Transnational Challenges and Future Security Cooperation', p. 12.

40 Edwards and Jennings, *Facing West, Facing North,* p. 13.

41 Jennings, 'Australia and Canada'.

42 Department of Defence, *Defence Issues Paper 2014,* p. 16.

43 Jennings, 'Australia and Canada'.

44 Abbott, 'Address to the Australia-Canada Economic Leadership Forum'.

The Changing Role of Intelligence within Military Decision-Making

Dr Dirk Maclean
Squadron Leader Charles Vandepeer, Royal Australian Air Force

Introduction

The intelligence function in Air Force is going through a period of rapid expansion and change. New platforms and capabilities, such as remotely-piloted aircraft and the integration of intelligence, surveillance and reconnaissance (ISR) into one operating concept, are redefining the position and role of intelligence within joint and combined air operations.

One aspect of this redefinition is the relocation of military decision-making, much of which will now take place within the ISR enterprise itself. The direction of collection assets and the processing, exploitation and dissemination of information in near-real time will increasingly act as the driver of targeting and tactical decisions. The primary focus of intelligence will shift from providing 'decision support' for operations to the making of operational decisions within its own sphere.

This new position turns the spotlight on to the quality of decision-making within ISR missions themselves. The requirement will be for rapid decisions, in near-real time, within a complex and dynamic environment, often with extreme consequences and involving teams of specialists in geographically-separate locations. This raises a whole new set of challenges if catastrophic failures are to be avoided and the full potential of ISR capabilities are to be realised.

Fortunately, Air Force intelligence is not the only domain faced with this challenge. Ensuring the quality of decision-making has been a longstanding concern for all branches of the military, and one that is shared across a number of civilian sectors facing similar dilemmas, such as emergency services, medicine, nuclear power plant operation, air traffic control and the aviation industry, collectively known as 'high-reliability organisations'.

The conclusions from recent research into decision-making across these sectors converge in a number of important ways and provide the foundation for a guiding framework that can minimise the risk of catastrophic error. This framework, titled 'high-consequence decision-making', incorporates a range of initiatives including training programs, management systems and an organisational culture suitable for meeting the challenges posed to Air Force intelligence by this new situation.

The traditional approach

Traditional approaches to military decision-making have centred on giving the process a rational, analytical structure. The analytic approach seeks consistency in the quality of outcomes through the adoption of a consistent method.

This is a direct application of classical 'rational choice' theory which dominated thinking around decision-making until the emergence of the 'naturalistic' decision-making school in the late 1980s. In a military context, rational choice theory underpins decision tools, such as the military appreciation process, and is generally considered to work best for relatively straight-forward tactical situations at small-unit level.

However, even within such a narrow field of application, the assumptions that underlie this model can be misleading, which helps to explain why, in practice, very few battlefield decisions are reached in such a structured manner. In reality, decision-making looks quite different and this simple observation has been the guiding impetus behind the new approaches that have emerged out of the naturalistic decision-making school.[1]

An important advance has been to redefine what a decision is. Traditionally, decision-making has been understood as an event, a pause in the flow of a situation where the decision-maker selects a course of action from alternatives, after which the flow restarts. At first glance, many military decisions appear to take this form. A classic example was the decision to launch an anti-air missile by the USS *Vincennes* in 1988, resulting in the shooting down of a civil airliner, Iranian Airlines flight 655. It was this incident that triggered the US Navy's 'Tactical Decision Making Under Stress' (TADMUS) project, the first serious investigation into military decision-making motivated by the desire to avoid such a catastrophic error happening again.[2]

Critical decisions of this nature—to go or not go, launch or not—often made in a split second, offer little to work with. Operators can be trained to cope with the stress of the moment, they can be given checklists and procedures, and they can practise and train using simulations. But none of these offers any real guarantee against high-consequence mistakes. The investigation into the shooting down of a Libyan airliner by Israeli Air Force fighter aircraft in 1973 found that the actions of the pilots were perfectly reasonable given the situation as they understood it; procedures had been followed, all available safeguards applied, and yet the outcome was a tragic and unnecessary loss of life.[3]

Fortunately, the situation is not so bleak. As the TADMUS project showed, it is not necessary to focus simply on the final decision event. In the case of the *Vincennes*, long before the final decision to launch or not, a whole series of earlier decisions, developments, actions and responses had taken place as the crisis unfolded over a number of hours. This broader perspective provides an opportunity to understand the process as a whole, and find areas where improvements can be made, mistakes avoided and best practices applied. Erik Hollnagel goes so far to suggest that decisions are in reality only 'attributed after the fact', and that it is more useful to think of decision-making as a continuous 'activity'.[4]

Situation assessment – the foundation of good decision-making

Understanding decision making as a continuous activity, set within a team and organisational context, allows the possibility for the process to be properly established, monitored and fine-tuned in real time, well before any final action has to be taken with potentially catastrophic consequences.

The key element shifts from the point of decision to the assessment of the situation on which those decisions are based. Situational awareness, leading to situation assessment, becomes the critical component of successful decision-making. Once this is done, the selection of an appropriate course of action is relatively straight forward, the decision makes itself.

This is helpful for understanding what went wrong in the case of the Libyan airliner, where both the Israeli Air Force pilots and the Libyan airliner's flight crew were acting in a fully logical and rational manner but on the basis of very different interpretations of the situation and the significance of each other's actions. In this instance, the predominant cause of the tragedy was a failure of communication as opposed to faulty decision-making.

This perspective also helps clarify what it is that sets experienced decision-makers apart from inexperienced ones. Successful decision-making is the product of streamlined cognitive processes that set aside irrelevant data, recognise familiar patterns, identify deviations from the norm, and are able both to anticipate problems and foresee the outcomes of particular actions.[5] On this basis, expert operators are able to quickly narrow down their options to one or two, and highlight the key points that will swing the decision one way or another.

Intuitive decision-making of this kind, therefore, rests on pattern recognition and the formation of mental models in order to arrive at a situation assessment in a short space of time, foregoing the need for lengthy analytic procedure. As the TADMUS project also revealed, intuitive decision-making centres on the creation of competing narratives.[6] Decision-makers create stories that cover over gaps in the information available and generate expectations as to what is likely to happen next, which can then be confirmed or refuted as events unfold, in much the same way as scientific theories generate new hypotheses that can then be tested by further observations.

In a separate incident from *Vincennes* and Iranian Airlines flight 655, the decision by the Captain of another US Navy AEGIS cruiser not to open fire on two Iranian Air Force F-4s operating in an aggressive manner is instructive. The decision not to engage was based on a judgment that their actions were better explained by a narrative that they were harassing his ship rather than a narrative in which they were attacking it.[7]

Mobilising critical thinking

The use of critical-thinking skills in this way is also essential in order to avoid some of the common errors that are known to arise when pattern recognition is the main input into the decision-making process. Research has identified a whole number of errors or biases that can lead to faulty reasoning. For example, an 'availability bias' reflects a tendency for 'recent or salient experiences to influence the choice of a diagnosis', while a 'confirmation bias' is where evidence that conflicts with a situation assessment already made is discounted or explained away.[8]

The use of mental models to understand reality is particularly prone to problems with confirmation, as models generate certain expectations, which is part of their function, and the decision-maker then actively seeks information confirming those expectations. A bias of this nature was the main explanation for the 1978 Chesapeake Bay collision investigated by Charles Perrow. The Captain of the US Coast Guard vessel *Cuyahoga* failed to take into account mounting evidence that his interpretation of an oncoming ship's behaviour and intentions was fundamentally flawed. As a result, the Captain turned his ship into the path of an oncoming cargo vessel, resulting in the sinking of the *Cuyahoga* and the death of 11 crew members.[9]

Perrow's research forms part of an important body of literature in the safety management field that sheds considerable light on the decision-making processes that result in catastrophe.[10] Among this work is Dorner's classic study, where he showed that 'failure does not fall like a bolt from the blue, it follows a logic'.[11] By tracing this logic, it is possible to create safeguards and design warning indicators to prevent a decision-making process leading to an obvious path to failure.[12]

The need for a critiquing function emerges from all the research strands that have investigated the dynamics of effective rapid decision-making processes. Not only systems theory but the safety management literature, and studies of aviation, medicine, emergency services and other civilian sectors demanding 'high reliability', as well as the military's own TADMUS project, all converge on one idea. Military decisions are best understood not as split-second events or 'moments of truth' but as ongoing activities within which team-based critical thinking can and does play a vital critiquing role in ensuring the quality of the decision-making process.

These studies have succeeding in stripping away much of the mystery that once surrounded intuitive decision-making and have managed to identify the key elements that combine to make for effective decisions, as well as the warning signs that indicate a process is seriously off track and on a course to disaster. This in turn creates the possibility for a quality control procedure to be built into the process itself. Without having to trade off quality for speed, the process can have a 'guardian'.

If decisions are not isolated events but a series of interconnected actions, then new additions to the series can be checked for consistency with previous ones and the way these earlier decisions have had an impact, intended or unintended, on the situation as it unfolds. In this way, conflicting

effects, unnecessary duplication, distraction from the main task at hand, and errors of omission, can be detected and avoided in real time.

If a mental map, model, analogy or narrative is being used to form an assessment of the situation, this can be measured against the standards of critique outlined by TADMUS. Are its assumptions reasonable, its conclusions valid, does it make sense, is it plausible? Or does it display some of the known pitfalls in recognition-based thinking, such as the availability or confirmation biases? How effective are the information management processes being employed? What do information requests reveal about a decision-maker's thinking and what do they suggest about the way the problem has been defined? Is there too much information available, causing overload and degrading cognitive capabilities, or too little, with dangerous blind spots? And as a mission proceeds, is the desired end-state still desirable, has it been superseded by events, are there unintended consequences of previous actions, or have new factors intervened?

It is not reasonable, or necessary, to expect the decision-maker to take on these critiquing functions and monitor the quality of the decision-making process across all its elements. Instead, a better solution is indicated by the principle underlying 'crew resource management', where all members of the flight crew act as 'guardians' of the decision-making process. This is also the approach considered as best practice in incident management, where a team member is given no specific area of responsibility but serves only as a 'process guardian', with an intimate knowledge of the plans, procedures and resources available to the team.

Intelligence in ISR

The changing role of intelligence can be most clearly seen in the development of an ISR capability and, in particular, the 'processing, exploitation and dissemination' (PED) function, which is designed to 'better meet the specific demands of air warfare, which is characterised by quick, decisive and focused engagements and thus requires time-critical, dynamic and instinctive information and intelligence support'.[13]

Airborne ISR platforms and the PED function have been a feature of ADF operations in Afghanistan, with a view to providing information superiority, enhanced situational awareness and decision superiority. PED is already forming an integral component of high-consequence decision-making and the expectation is that this will continue into the future. The quality of decision-making processes within the PED function itself, therefore, will more and more influence the success or failure of operations.

The Air Force's ISR operating concept leaves it open as to whether operations are driving intelligence or intelligence is driving operations or if, in fact, intelligence is now operations. This same ambiguity is structured into the PED function, which in practice—according to RAAF doctrine—is 'neither linear nor cyclic; it more accurately represents a set of interdependent functions that must be performed, often simultaneously, to deliver effective ISR'.[14]

The PED function explicitly places intelligence analysts inside the decision-making sphere, with analytical judgments directly influencing tactical and operational decisions within the battlespace. In the US, the functional capability has been incorporated into the 'Distributed Common Ground System' (DCGS), which provides 24-hour analysis of data from ISR assets in near-real time. The wide range of roles and responsibilities allocated to intelligence personnel assigned to this system has been described as follows:

> [Intelligence personnel] are involved in every step: planning, execution and evaluation. Whether locating improvised explosive devices on a convoy route, tracking a vehicle through heavy traffic, observing patterns of life for a person of interest, helping identify enemy targets for a kinetic strike or doing battle damage assessment, these airmen are a foundational part of the military's ISR enterprise. Furthermore, in addition to analyzing the data, they are constantly involved in coordinating and communicating with the aircraft's pilots, sensor operators, command centers, and troops 'downrange'. In some cases, even sensors on aircraft thousands of miles away are directly controlled from the DCGS.[15]

Such a heavy workload and responsibility comes with challenges, not least the combat-related risk factors that include critical decision-making relating to targeting and enemy identification; provision of timely and accurate information to protect troops on the ground; and regular exposure to videos and images of death and destruction. The growing demand for DCGS intelligence support, the nature of the mission, sustained operations and personnel shortages, have all led to concerns over the potential for burnout for intelligence analysts.[16] These issues have the potential to negatively impact on the quality of decisions being made by the personnel involved.

The RAAF is set to establish a centralised, near real-time distributed ISR PED capability in the form of a 'Distributed Ground System-Australia'. It will operate in a similar manner to the US construct, providing an opportunity to learn from their experience.[17] It will have numerous key and influential decision-making positions assigned to intelligence personnel, including ISR mission commanders, PED crew commanders, PED analysts and ISR liaison officers (embedded with end-user units). As with the US example, Australian intelligence personnel will be involved in the execution of missions, with the ISR mission commander playing a pivotal role.

This is an expansion of Air Force intelligence and a redefinition of its role in operations. The PED and ISR constructs require new types of relationships inside the ISR process and between intelligence and operations personnel. A key feature of these relationships is the distributed nature of teams, made up of specialists heavily dependent on one another, who need to understand their particular contribution at all times during the life of the ISR mission to achieve overall success.

Critical to this is the development of situational awareness across the team that both shapes and reflects the commander's intent, in turn facilitating rapid decentralised decision-making on the basis of a common understanding of the battlespace. This is a difficult challenge, all the more so as teams can be switched between entirely different theatres. But it is essential to cope with time-critical, complex decision-making with potentially extreme consequences.

Process guardian: individual, team and culture

The difficulty and complexity of the task calls for checks and balances, to guard the process from common sources of error identified within the literature. A 'process guardian', responsible for the quality of the process by which decisions are being made, can take the form of an individual, team or culture.

At the individual level, one approach used in incident management is to appoint a deputy whose main responsibility is to ensure the quality of the decision-making process. At the team level, members are responsible for identifying and raising concerns and for the accuracy of the team's overall situational awareness, in the same way the Air Force already employs crew resource management in manned platforms.

In terms of culture, drawing on best practice in high-reliability organisations, the approach would be to instil an attitude that rejects complacency, recognises the inevitability of mistakes and failures, and seeks continuous improvement and learning. Arguably, this is the most difficult form of process guardian to implement but is ultimately the most important.

This is built on the understanding that decision-making is not an event but a process, and the key is to ensure the quality of that process. The result is to take the emphasis away from individuals, selected on the basis of personality traits considered to provide them with the capacity for taking rapid, high-consequence decisions. Instead, the quality of decision-making is assured by team-based and organisational processes in the same way that crew resource management and high-reliability organisations have evolved away from sole reliance on a single pilot or operator, based on some hard-won lessons in aviation and plant safety.

ISR operations will need to rest on an understanding of the pivotal role played by effective team processes in building shared situational awareness—and develop ways to overcome the particular obstacles to team formation posed when these teams are geographically distributed.

Operators will also need the ability to mobilise critical-thinking skills in order to arrive at accurate assessments of the situation as it unfolds, avoiding known traps and pitfalls, and with the agility to rapidly reassess the status of the mission as the circumstances require. This ability will also rely on a team environment that allows space for dialogue, divergent thinking and the challenging of familiar assumptions.

These requirements in turn call for the shaping of a supportive culture across the intelligence function, so that individual operators and teams can develop the appropriate skills and behaviours that minimise the potential for catastrophic error. This requires leadership commitment, as well as an investment in appropriate training programs which develop the key components that make up high-consequence decision making.

They also highlight the case for a process guardian, both in the sense of an individual role within the mission structure but also as a safeguard arising out of team processes, organisational culture and through the development of management systems and procedures. They will have the task of assuring the quality of decision-making—without compromising speed or reducing the promise of decision superiority—that guides the ISR operating concept and is driving the changing role of intelligence within military decision-making. This process has already begun.

Training for high-consequence decision-making

In 2014, Information Warfare Wing commenced a pilot training program aimed at introducing the principles of 'high-consequence decision-making' as part of initial employment training for Air Intelligence Officers and Air Intelligence Analysts. As at September 2014, 36 such personnel have undertaken this scenario-based, interactive training.

The training raises awareness of the risk of catastrophic failure and the impact that decisions from junior through to senior levels can have in minimising or increasing risks. It includes an in-depth examination of past tragedies, such as the shooting down of Iranian Airlines flight 655 in 1988, and the Black Hawk 'friendly fire' incident in northern Iraq in 1994, as well as more positive examples of high-consequence decision making such as the conduct of Operation ANACONDA in Afghanistan during 2002.

Participants in the program are also taken through a structured decision-making process that emphasises the key elements of situational awareness, situation assessment, appreciation of commander's intent and rules of engagement, as well as an anticipation of the consequences that will flow from decisions taken. The aim is to give intelligence officers and airmen/women the ability to determine where high-consequence decision-making processes are on track or else at an elevated risk of failure, and the confidence to step in and prevent a catastrophic outcome from occurring.

Conclusion

As the ADF is in the early stages of ISR operations and developing a PED capability in the form of a Distributed Ground System-Australia, this is a timely and relevant discussion. It allows the opportunity to incorporate the lessons and best practices from a wide range of areas that have faced the same challenges in terms of rapid decision-making with high consequences, and apply these through the high-consequence decision-making program. Above all, it gives Air Force Intelligence the tools with which to minimise the ever present risk of catastrophic error.

Dr Dirk Maclean has a background in emergency services and has acted as a consultant and trainer for incident and crisis management teams across the corporate sector in Australia, New Zealand, China, India, and PNG. Dirk has an MBA and a PhD from La Trobe University and has written and lectured on the management principles behind 'High Reliability Organisations'.

Squadron Leader Charles Vandepeer is a Reserve Intelligence Officer with the RAAF, having gained operational experience in Southeast Asia and during deployments in the Middle East as part of Operations CATALYST and SLIPPER. In his civilian career, he is an Operations Research Scientist as well as a Visiting Research Fellow at the University of Adelaide, where he completed his PhD into concepts of threat within intelligence analysis. He is the author of 'Applied Thinking for Intelligence Analysis', published by the Air Power Development Centre.

NOTES

---

1 Gary Klein, Judith Orasanu, Roberta Calderwood and Caroline E. Zsambok (eds.), *Decision Making in Action: models and methods*, Ablex: Norwood, New Jersey, 1993, p. 26.

2 Marvin S. Cohen, Jared T. Freeman and Bryan B. Thompson, 'Integrated critical thinking training and decision support for tactical anti-air warfare', in Center for Advanced Command Concepts and Technology, *Proceedings of the Third International Command and Control Research and Technology Symposium*, National Defense University: Washington DC, June 1997.

3 Klein *et al*, *Decision Making in Action*, p. 30.

4 Erik Hollnagel, 'Decisions about "what" and decisions about "how"', in M. Cook, J. Noyes and Y. Masakowski (eds.), *Decision Making in Complex Environments*, Ashgate: Farnham UK, 2006, p. 5.

5 Monique Cesna and Kathleen Mosier, 'Using a Prediction Paradigm to Compare Levels of Expertise and Decision Making Among Critical Care Nurses', in H. Montgomery, R. Lipshitz and B. Brehmer (eds.), *How Professionals Make Decisions*, Lawrence Erlbaum: New Jersey, 2005, p. 109.

6 Cohen *et al*, 'Integrated critical thinking training and decision support for tactical anti-air warfare'.

7 Marvin S. Cohen, Jared T. Freeman and Bryan Thompson, 'Critical Thinking Skills in Tactical Decision Making: a model and a training strategy', Cognitive Technologies: Arlington, 1998, available at <http://www.cog-tech.com/papers/chapters/tadmus/tadmus.pdf> accessed 16 October 2014.

8 Klein *et al*, *Decision Making in Action*, p. 36.

9 Kevin Burns, 'Mental Models and Normal Errors', in Montgomery *et al*, *How Professionals Make Decisions*, pp. 15-6.

10 Charles Perrow, *Normal Accidents: living with high-risk technologies*, Princeton: New Jersey, 1999.

11 Dietrich Dorner, *The Logic of Failure: recognising and avoiding error in complex situations*, Metropolitan Books: New York, 1996, p. 10.

12 Dietrich Dorner, P. Nixon and S.D. Rosen, 'Human factors in hazardous situations', *Biological Sciences*, Vol. 327, No. 1241, 1990, pp. 463-73.

13 RAAF, *The Air Force Approach to ISR, Intelligence, Surveillance and Reconnaissance Operating Concept*, Air Force Headquarters: Canberra, March 2013, p. 2

14 RAAF, *Intelligence, Surveillance and Reconnaissance Operating Concept*, AAP 1001.3, Air Force Headquarters: Canberra, October 2011, p. 99.

15 John K. Langley, *Occupational Burnout and Retention of Air Force Distributed Common Ground System (DCGS) Intelligence Personnel*, RAND Corporation: Santa Monica, 2012, p. 9.

16 Langley, *Occupational Burnout and Retention of Air Force Distributed Common Ground System (DCGS) Intelligence Personnel*, p. 28.

17 RAAF, *The Air Force Approach to ISR, Intelligence, Surveillance and Reconnaissance Operating Concept*, p. 1.

Opinion piece

Energy Competition in the South China Sea: a front-burner issue? [1]

Dr Euan Graham, Nanyang Technology University, Singapore

Introduction

The recent confrontation between Vietnam and China over the latter's deployment of a deep-water drilling rig in disputed waters has refocused the spotlight on energy in the South China Sea. How important is it as a driver in China's South China Sea policy? To what extent is competition over seabed hydrocarbons compounding tensions between China and Southeast Asian territorial claimants?

In fact, political and strategic motivations almost certainly took precedence over energy considerations in the decision to deploy China National Offshore Oil Corporation's (CNOOC's) deep-water platform west of the Paracels in early May 2014. Nevertheless, the imperative to exploit seabed energy resources has received greater attention within China's overall South China Sea policy in recent years.

China's pursuit of maritime power

China is now the world's largest oil importer, a simple fact that has increased its exposure to political risk in the Middle East and Africa, and to potential disruption in transit, as well as growing competition to secure new upstream resources. China is thought to be topographically disadvantaged when it comes to exploiting its shale deposits. Exploiting offshore energy within China's 'near seas' is therefore seen as an attractive option from a supply-security perspective against projections for future demand growth.

A heightened focus on energy exploration and securing a greater share of oil and gas resources in the South China Sea, unilaterally if necessary, has emerged in internal Chinese policy debates over the past five years. This has fed into a major capability upgrade for China's state-owned energy conglomerates, including acquisitions of deep-water rigs, seismic survey vessels and support craft that are now becoming operational. Alongside expansion of the merchant fleet, ports infrastructure and naval modernisation, the development of the offshore energy sector can be considered as another key pillar in the Chinese leadership's pursuit of comprehensive 'maritime power'.

CNOOC first announced plans to invest US$30 billion on deep-water projects, over two decades, in 2009. A second deep-water drilling platform is scheduled for completion in 2016 and is specifically designed to operate in the South China Sea. For CNOOC and China's other state-owned energy firms, this brings a step-change for exploration and production activity in the South China Sea at large. In this context, the stand-off with Vietnam is more likely to be a rehearsal than an isolated incident.

As the number of China's deep-water rigs increases, their deployment further afield is likely to become more common, although the logistical and security challenges for long-distance exploration and production operations in the southern portions of the South China Sea are significant. This helps to explain the choice of the Paracels for the first deployment, being relatively close to Hainan.

Hydrocarbon deposits

The growth of China's offshore exploration and production capabilities has proceeded hand-in-glove with the expansion and centralisation of its maritime law enforcement capacity, which is tasked with protecting these high-value assets as they venture further out into disputed waters. A pattern of close cooperation was evident throughout CNOOC's deep-water platform's turbulent six-week deployment, in which law enforcement vessels provided an outer security cordon around an inner core of support craft surrounding the platform itself.

That the South China Sea is energy-rich is not in doubt, including oil and gas fields off China's Pearl River Delta and Hainan. But the underlying geology points to a concentration of hydrocarbon deposits around the periphery and the sea's southern half in particular, economically advantaging Malaysia, Brunei, Indonesia, Vietnam and The Philippines.

A 2010 US geological survey estimated the untapped energy potential of the South China Sea at 11 billion barrels of oil and 145 trillion cubic feet of gas. Much larger estimates by Chinese sources remain uncorroborated. Deep-water areas of the South China Sea are abundant in methane hydrates but the recovery of natural gas from these deposits is a long-term proposition at best.

While a major strike in unsurveyed portions of the South China Sea cannot be ruled out, industry analysts question the energy potential of the Spratly and Paracel Islands and surrounding waters. This may have the effect of drawing China's exploration and production activity southwards over time, raising the stakes of further confrontations and stand-offs in the EEZ of Southeast Asian littoral states, where these overlap with China's ambiguous dashed-line claims.

Malaysia, Brunei and Indonesia have been producing energy in the southern South China Sea for decades, while Vietnam and The Philippines are newer entrants. Vietnam has moved rapidly to exploit offshore energy within its EEZ. Owing to large discoveries in the Nam Con Son and Cuu Long basins, Vietnam is a petroleum exporter but still imports refined products. The Philippines is pumping gas from the Malampaya field and has made new discoveries at Reed Bank.

Impact of energy exploration

Most Southeast Asian producers rely on joint ventures with foreign partners, although Malaysia's Petronas stands out as a global player with diverse upstream and downstream investments. China's energy companies also operate globally on a for-profit basis, and their profile as investors in Southeast Asia is naturally expected to grow.

However, political and strategic imperatives can take precedence especially within the 'near seas', as was the case with the deployment of CNOOC's deep-water platform in May. Equally, the decision to withdraw prematurely, in July, suggests a political motive although such signals have to be inferred.

Vietnam has sought a deliberately diverse portfolio of joint venture partners, granting block concessions to Russian, Indian, Malaysian, US and European-listed energy firms, with the implied aim of internationalising its maritime claims. Vietnam has recently offered India's ONGC-OVL five additional oil and gas blocks in the South China Sea for exploration, although the company's existing Vietnamese concessions have yielded disappointing results.

A reactive dynamic can therefore be seen at play in the South China Sea, whereby energy exploration by Vietnam and The Philippines has fanned China's fears of 'losing out', prompting a significant policy shift since 2009 away from the joint development paradigm to unilateral exploration and production, including within disputed waters. To this can be added the physical disruption of energy surveys undertaken by foreign firms exploring under licence within the EEZs of Vietnam and The Philippines.

Vietnam and The Philippines are concerned that the geographical pattern of maritime incidents and the growing presence of Chinese vessels further south in the South China Sea owes at least in part to the proximity of oil and gas. The Philippines recently protested against the regular presence of Chinese survey vessels in Reed Bank, alleging that this contravenes innocent passage within its EEZ.

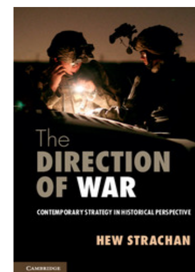
Euan Graham is a Senior Fellow in the Maritime Security Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. From 2004-10, Dr Graham was Senior Research Officer for the UK's Foreign and Commonwealth Office, serving as the lead analyst for the Korean Peninsula and Japan, before heading the Southeast Asia and Pacific Research Group.

NOTES

[1] This is an edited version of an article published as RSIS Commentary No. 179 on 11 September 2014 by the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. It is reprinted with permission of RSIS.

Book reviews

The Direction of War: contemporary strategy in historical perspective



Hew Strachan
Cambridge University Press: Cambridge, 2013, 322 pages
ISBN: 978-1-1076-5423-5
£18.99

Reviewed by Lieutenant Colonel Gavin Keating, Australian Army

US President Obama concerned many in the international community when he admitted in a late August 2014 news conference that 'we don't have a strategy yet' for dealing with the growing power of the Islamic State in Syria and Iraq. *The Washington Post*, in late September, subsequently described as 'stunning' the swiftness of the US leap from 'no strategy' to a full battle plan.

Any reader of Hew Strachan's *The Direction of War: contemporary strategy in historical perspective* will be well placed to probe the many nuances surrounding the President's original admission and subsequent events. Strachan is an internationally-renowned military historian and currently the Chichele Professor of the History of War at the University of Oxford.

His latest publication is a collection of articles and lectures whose central theme is 'strategy, what we understand by it, and how that understanding has changed. It rests on the presumption that strategy is useful, and even necessary, if states are to exercise military power'. As the book's subtitle implies, Strachan's work is heavily influenced by his belief that historical context is require to distinguish what is really new in the West's experience of war in Iraq and Afghanistan over the last decade, and what represents a firm continuity with the past.

One of Strachan's key messages is that strategy faces an 'existential crisis' because its definition has gradually become so broad that it is now widely misunderstood by both political leaders and their military advisers. The early parts of the book trace this erosion in clarity. For Clausewitz, strategy was 'the use of battle for the purposes of the war' which, until the end of the First World War, was an understanding commonly held in all European armies.

However, in seeking to fully explain the reasons for Germany's defeat during this conflict, beyond those found on the immediate battlefield, the term began to widen. Concepts such as 'grand' or 'national' strategy emerged to describe the development of the national policies required to coordinate and apply all facets of national power. Perhaps not surprisingly, given the scope of the Second World War, 'strategy and policy [after 1945 became] conflated in people's minds'.

This divergence from the original meaning was further reinforced by the peculiarities of the Cold War, with its focus on deterrence, wherein the modern understanding of strategy became further removed from the realm of actually fighting on the battlefield. Strachan believes that 'armies and their generals lost their way' during this time. The 'invention' by the US military of the so-called operational level of war during the 1980s was a response to this trend but introduced the belief that this arena could be isolated from policy constraints.

The dangers of this mutation became apparent in the sort of thinking that produced the 'Powell doctrine', which was rapidly discredited when confronted by the pressures placed on the US military by its political masters since 2001. The end result of this loss in definitional clarity has been that most of the parties involved with discussing war in contemporary Western society do not actually understand strategy's real meaning.

Strachan is a firm advocate that Clausewitz remains highly relevant to understanding strategy in the modern world—indeed, one of the chapters of the book is titled 'The Case for Clausewitz: reading *On War* today'. He takes umbrage, however, at those who have only superficially read this classic text or unthinkingly interpret it through their own world views. He notes that Clausewitz's much-quoted dictum that 'war is the continuation of politics by other means' needs to be carefully considered. In his view, *On War* presents two different and potentially opposing views of the relationship between war and policy.

The first, as indicated by the quote, implies that policy controls, guides or even limits war—something which sits well with liberal and rationalist thought. For Strachan, this is 'a statement about how governments might use war; it is not a statement about the nature of war'. The second view reflects the fact that this theoretical reality does not sit comfortably with observed practice. While ideally both war and policy should be related, they are very different and, at times, conflicting entities.

War has its own nature and this can, and does, serve to shape and change policy through complex and ongoing interactions. Strachan concludes this particular chapter by citing another famous Clausewitzian dictum concerning the critical requirement for the statesman and commander to determine 'the kind of war on which they embarking; neither mistaking it for, nor trying to turn it into, something that is alien to its nature'. He further notes that while assessing the character of an individual war is properly within the remit of the military professional, the ensuing conclusions have profoundly political repercussions.

An additional theme that emerges in *The Direction of War* is the critical importance of specifically addressing the dynamic relationship between strategy and policy. In simple terms, this is the relationship between a nation's military commanders and its political leaders. Historically, the management of this relationship has been potentially fractious. Strachan argues that 'the principal purpose of effective civil-military relationships is national security: its output is strategy'.

Western democracies, in their concern about maintaining civil primacy over their military forces, tend to forget this equation. As Strachan suggests, strategy is the 'interface between operational capabilities and political objectives: it is the glue which binds each to the other and gives both sense'. It is an inherently iterative process of dialogue, where ultimately compromise must be reached between 'the ends of policy and the military means available to implement it'.

The book's survey of US and UK performance in the wars in Iraq and Afghanistan strongly suggests that this process of dialogue is largely broken. Strachan believes that politicians should better empower their generals to contribute to the dialogue so necessary for the creation of successful strategy. In his view, the real danger to Western democracies is not military coups but 'the failure to develop coherent strategy'.

Ultimately, strategy 'is designed to make war useable by the state, so that it can, if need be, use force to fulfil its political objectives'. While this is superficially straight forward, Hew Strachan's *The Direction of War* makes it abundantly clear that this process is anything but simple. Given his many criticisms of the current state of strategy in the Western world, it would be interesting to know what Strachan made of President Obama's recent 'no strategy' statement. Tellingly, in January 2014, Strachan told one media organisation that Obama's failures in Afghanistan and Syria had shown that he was 'chronically incapable' of formulating military strategy.

China's Naval Power: an offensive realist approach

Yves-Heng Lim
Ashgate: Farnham UK, 2014, 234 pages
ISBN: 978-1-4094-5184-6
£65

Reviewed by Squadron Leader Travis Hallen, RAAF

China's Naval Power: an offensive realist approach is a surprisingly engaging and interesting analysis of the sources of China's naval modernisation. 'Engaging' because, despite its foundation in international relations theory, the book does not read as a dry academic treatise. Rather, it provides an easy-to-follow and contextualised overview of different international relations theories and their relevance to understanding China's rise. 'Interesting' because Yves-Heng Lim's analysis draws on the political and strategic writings of Chinese officials and theorists, thereby providing an insight into the indigenous sources of Chinese naval development and innovation. Accordingly, it is a useful addition to any China watcher's library.

The author is well placed and qualified to write on this topic. An assistant professor at Taiwan's Fujen Catholic University, Lim has authored numerous articles on the implications of China's rise in Asia. His proximity to his chosen subject, coupled with a PhD from Peking University (co-delivered by the University of Lyon), confers on Lim a degree of authority not enjoyed by many US or Australia-based China watchers. Moreover, his language ability has provided Lim access to a range of primary resources not available to other commentators. Together with the book's excellent structure and easy-to-read prose, the author's qualifications to write on the subject ensure the argument he presents is compelling.

The book's central thesis is simple: 'the rapid and ongoing modernisation of Chinese naval forces stems primarily from China's need and ambition to secure a hegemonic position in the East Asia region'. This is offered as an alternative to reasons Lim identifies as generally used to explain the rise of the People's Liberation Army-Navy (PLAN): namely, the desire to retake Taiwan, the protection of Chinese sea lines of communications (SLOC), and naval nationalism. To support this thesis, Lim draws on two theories: Posen's theory on military innovation and Mearsheimer's offensive realism.

Although it is not referenced in the text itself, the book's back matter identifies Posen's theory on the sources of military doctrine as a key theoretical inspiration. This theory holds that 'statesmen will intervene in the doctrines of their military organisations as part of an overall pattern of balancing behaviour'. Civilian intervention ensures the integration of military innovation with grand strategic objectives. Lim makes one critical modification in his application of this theory, replacing the defensive realist notions of balance of power with the offensive realist concept of power competition aimed at hegemony. According to Lim, it is this power competition that is driving the development of China's sea denial and sea control capabilities, and the main focus of the book.

Lim supports his thesis by exploring the shift in modern Chinese naval strategy and delving into the particulars of PLAN modernisation. China's naval strategy took an offensive turn in the 1980s, away from the Mao-era guerrilla war on the water towards an 'active defence, near sea operations' focus. This shift in strategy is reflected in the types of vessels being acquired and their potential utility for the attainment of sea control.

Highly-capable anti-air and anti-surface warfare capabilities, together with anti-ship cruise and ballistic missiles, and a growing fleet of modern diesel-electric submarines have, as Lim rightly asserts, greatly increased China's ability to 'control the sea in the first island chain', and rendered 'transoceanic power projection hazardous, if not impossible, for the United States'. In contrast, there is a conspicuous lack of focus on anti-submarine warfare, a critical capability for the protection of China's SLOC. Additionally, the type of amphibious capabilities provided by the new Yuzhao-class landing ships and the decision to assign them to the South Sea Fleet indicates,

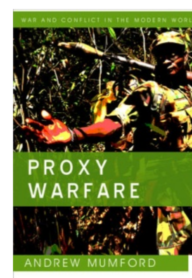
according to Lim, that they are intended to support the seizure of territory and support control of the South China Sea, not Taiwan.

Lim contends that by developing the ability to deny American naval access to the region, China can attain dominance in the local maritime commons and thereby achieve regional hegemony. Hegemony, a key grand strategic outcome for the offensive realist, would enable the resolution of lesser strategic goals, such as the integration of Taiwan and the imposition of a regional regime conducive to Chinese interests. Lim's well structured examination of this relationship between the pursuit of a long-term goal of regional hegemony and the satisfaction of China's short-term 'core interests' supports his assessment that China's naval modernisation program appears to be driven by a clear understanding of why and how military doctrine should be integrated with grand strategy.

Where Lim's analysis falters is in his assessment of the sources of this drive. Central to Posen's theory is the premise that it is through civilian intervention that military innovation integrates with grand strategy. Lim, however, identifies Admiral Liu Huaqing as a major driving force behind the shift in PLAN strategy and capabilities. This suggests that it is the military that is the master of its own destiny. If this is true, then it is likely that China's naval modernisation is a manifestation of naval strategic thinking that currently correlates to but is not integrated with a grand strategic goal of regional hegemony. If this is the case, it is possible that PLAN development will begin to diverge from the requirements of grand strategy. This would undermine Lim's central thesis.

Lim provides a compelling argument that innovation in China's naval capability and strategy is contributing to a grand strategic goal of achieving regional hegemony. However, the degree to which this is been driven by a civilian grand strategic vision, rather than being a manifestation of naval theory remains unclear. This critique of the theoretical processes of the work does not, however, detract from the book's insights. *China's Naval Power* is therefore highly recommended to the political scientist, military strategist and even the general reader interested in understanding the future of China's naval modernisation.

Proxy Warfare



Andrew Mumford
Polity Press: Cambridge, 2013, 180 pages
ISBN: 978-0-7456-5183-7
$31.95

Reviewed by John Donovan

Andrew Mumford, a Lecturer in Politics and International Relations at the University of Nottingham, has written a short survey of proxy warfare. He reviews the recent rise of proxy war, covering conflicts from the Spanish Civil War to recent days. Mumford notes that it is not only superpowers that have resorted to proxy war, as non-state actors like Hizballah have also found it useful. With the decline of traditional conflict, Mumford sees an increasing role for proxy war.

Mumford attempts to define proxy war, using the Spanish Civil War as an example. In that case, he sees Germany and Italy fighting a war of intervention, with their own military personnel deployed, while the Soviet Union fought a proxy war through its sponsorship of the International Brigades. His distinction, however, seems to lose its clarity when the early (advisory) period of the Vietnam War and the recent deployment of Chinese personnel into parts of Africa come under discussion, with both regarded as proxy wars.

Drawing a distinction between the deployment of formed military units and thousands of 'advisers' seems like a debate on the number of angels that can dance on the head of a pin—interesting to theologists but of limited practical value. His dismissal of the potential role of NGOs and the UN as participants in proxy wars also seems to discount too easily the effect of their

presence, which allows governments and their opponents to focus on fighting by relieving them of much responsibility for refugees and other casualties.

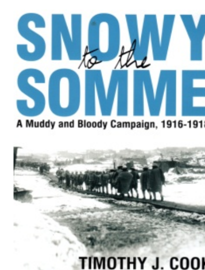
Mumford has chapters on the appeal of proxy wars, who engages in them, how they are fought, and the future and continuing appeal of proxy wars. There is some discussion of the rise of private military companies, with their perceived benefit of moving the political costs of casualties away from governments but, surprisingly, no mention is made of forces such as the French Foreign Legion or the Ghurkhas. Such forces also move the political pain of casualties elsewhere but they provide greater control to their sponsoring government.

Perhaps Mumford's clear disdain for companies such as Sandline and Blackwater explains his reluctance to look too closely there, albeit he does mention the possibility that the UN might at some stage have to consider the use of private military companies. In this context, some less developed nations already seem to use their armed forces effectively as UN mercenaries, deploying them to gain the payments that accrue from the UN.

Mumford forecasts more proxy wars in the future, as states become reluctant to commit their own troops to conflicts. Also, regional powers are now using proxy war more often. He sees the jihadist use of proxy wars as particularly concerning, because of the 'perpetuity of the jihadist interpretation of their struggle'. Those commanded by their religion to ensure its supremacy will, in his view, continue to fight an eternal holy war until victory is attained. This is not a happy prospect!

The book would be easier to read if Mumford did not employ numerous multi-syllable words where a few short ones would suffice. His propensity for complex academic language ('multitheoretical understanding' and 'relevance of certain tenets from alternative theoretical schools') and trite statements of the obvious ('calculations made by states and non-state actors … are predicated upon an inescapable acknowledgement of self-interest') also do not help. The occasional grammatical infelicity also jars ('hard' and 'soft' are not verbs). Overall, this is potentially an interesting book but it is not easy to dig the gems from the surrounding layers of over-burden.

Snowy to the Somme: a muddy and bloody campaign 1916-1918



Timothy J. Cook
Big Sky Publishing: Sydney, 2014, 397 pages
ISBN: 978-1-9221-3263-5
$30.00

Reviewed by Lex McAulay

Timothy Cook has presented a detailed look at the life and times of the 55th Australian Infantry Battalion AIF, 1916-1918. None of those veterans are with us but live on through the unit's war diary and the letters, diaries and post-war memoirs of the unit members.

The battalion's early experiences included the disastrous desert marches in March 1916 on the orders of General James Whiteside McCay (who found a scapegoat in Brigadier Godfrey Irving), a brief pleasant interlude on arrival in France, then the debacle at Fromelles. After recovery, the battalion took part in all the battles fought by the Fifth Division AIF, under the respected Talbot Hobbs after McCay was removed—Doignies, Bullecourt, Polygon Wood, Anzac Ridge, Wytschaete, Villers-Bretonneux, the battles of August 1918, Peronne and Bellicourt.

Some men survived battle after battle, bombardment after bombardment, while others disappeared in the mud and darkness. The wide-spread use of animals in modern warfare has

thankfully ended but the description of German artillery falling on a horse-drawn column, though a common event, is disturbing reading. The winner of the only Victoria Cross awarded to a member of the 55th, Private John Ryan, survived a fight with bayonet and bombs to clear a section of trench on 30 September 1918. The after-effects of war service on John Ryan serve as an example—by the time he returned to Australia he was an alcoholic and died destitute.

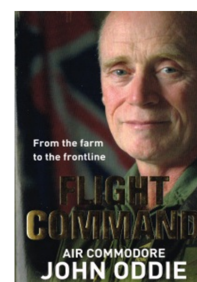
The battalion's last actions were at the Hindenburg Line, after which the AIF was at the end of its strength and badly in need of rest. C Company was commanded by a sergeant, and the English unit that replaced it was astounded to find so few representing a rifle company. The actions throughout are very well described and the maps—drawn by daughter Amelia—are good, though presented at right-angles to the text. The content is well supported by 17 maps, a roll of honour, summary of casualties, honours and awards, nominal roll, bibliography and extensive endnotes and index.

A strong thread through the pages is the contribution of personal experiences left by the battalion members of all ranks. These leave the reader in no doubt of the severity of the casualty rate, the frightful winter conditions and the constant attrition by German artillery. Given the education standards of 100 years ago, when secondary schooling was not common and university attendance rare, the powers of expression and grammar are impressive. When universities today are forced to provide courses in English expression and grammar to entrants who are incapable of written communication after 12 years of education, one wonders how today's soldiers might leave a record of their military experience, and if historians in 100 years will be able to present personal experiences as in this book.

Unit histories such as *Snowy to the Somme* reinforce the impression of the archives at the Australian War Memorial as a national treasure, complemented by collections at federal and state libraries. Regrettably, readers probably have personal knowledge of the wanton waste of personal memorabilia by families on the death of the veteran, when those items could be donated for use and appreciation by others.

Snowy to the Somme is a worthy addition to any collection of books on World War 1 and of battalion histories.

Flight Command



Air Commodore John Oddie, with Mark Abernathy
Allen & Unwin: Sydney, 2014
ISBN: 978-1-7433-1981-9
$32.99, 336 pages

Reviewed by Air Commodore Mark Lax, OAM, CSM (Retd)

Flight Command tells the story of a young farm boy who dreamed to fly and went on to higher things. It is autobiographical and early chapters tell of an upbringing in Skipton, Victoria and a desire to join the RAAF. Air Commodore John Oddie was to be successful and had a varied flying career, first on helicopters and then fixed-wing transports, before undertaking a series of wide-ranging deployments from the First Gulf War as a line pilot to Afghanistan as Australian Deputy Commander. Flying adventures are really only the prelude. John also held the important positions of Commander Air Lift Group and Director General Capability Development, which allowed him to make a tremendous contribution to the RAAF.

When I was asked to review *Flight Command*, my initial thought was 'oh no', not another memoir on how I won the war in X, Y and Z. Pleasingly, it is nothing of the sort. As the chapters unfold, the reader will come to realise the book has two themes: military leadership and the challenges a leader faces, and the need to recognise families and just how important they are to those who

serve. It is very much about the internal struggles of those placed in a position of authority and the responsibility they bear to those they command. It is also about families and those left behind; the silent and unheralded that wait for their loved ones' return. It is about the sadness and sense of personal loss when one of the team is lost. Their return starts with a ramp ceremony and tears.

The book is a snapshot of a service life and will be surprising to those who have not served. It is written to educate that audience and debunks the stereotypes of servicemen and -women played out by Hollywood and many facets of the Australian media. The story tells of the highs of service life as well as the lows, and will trigger similar memories for those who have worn a uniform. John goes at length to explain the physical, emotional and mental toll in dealing with death and destruction, and the reader can feel the palpable sense of despair particularly as John tells of trying to manage the disaster as one of the first responders to the destruction of Banda Aceh by tidal wave in 2004. He calls the chapter 'a tragedy beyond belief' and is an experience that clearly still haunts him today.

There is also much home-spun philosophy in *Flight Command* that a 35 year career teaches one but, as I read through, I thought there is perhaps too much self-deprecation, almost too much humility. I didn't agree with everything John espouses but, then why would I, it is not my story. A constant theme is the reconciliation of the human cost of operations against what he calls the benefits 'measurable and uncertain'—however, you do what your country needs you to do, like it or not. This clearly troubles John and, as he freely admits, no doubt contributed to later bouts of depression so clearly depicted by the portraits of him by war artist Ben Quilty whose pictures are included.

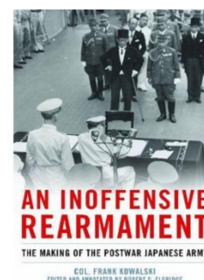
The book is 316 pages of text, as well as an index and 16 pages of colour photographs which aptly illustrate John's military life.

The book is as much an unloading from the heart, part of a healing process and a bridge to normality that many servicemen and -women like John feel they must cross. We all have our demons to exorcise and this I think is John's pathway. In his final paragraph, John asserts his aspirations for the book are:

> [T]hat the nature of military service in Australia be better understood as reflecting our society and its need for a confident future, that our military families will be better honoured in quiet ways and publicly for their support, and finally that our society better understands that military service is drawn from society to serve society.

I very much hope he succeeds.

An Inoffensive Rearmament: the making of the post-war Japanese Army



Frank Kowalski (edited and annotated by Robert Eldridge)
Naval Institute Press: Annapolis, 2014, 198 pages
ISBN: 978-1-5911-4226-3
US$37.95

Reviewed by Dr Russell Parkin, Australian Defence College

In June this year, Japanese Prime Minister Shinzo Abe introduced legislation that reinterpreted the so-called 'pacifist clause' in Japan's constitution. Article 9 has prevented Japanese forces from fighting overseas since the end of the Second World War and has been the bedrock of Japan's international relations since the 1950s.

The recent political turmoil in Japan over Abe's action provides an interesting contemporary context to Kowalski's *An Inoffensive Rearmament*. While the subject matter of the book is interesting enough in itself, the preface tells the intriguing story of how the original 1969 edition came to be written. The author specifically intended *An Inoffensive Rearmament* be translated into Japanese, the language in which it remains the standard reference on Japan's immediate post-war rearmament. Surprisingly, there was no English language edition until this version was published.

Over 15 concise and readable chapters, *An Inoffensive Rearmament* details the evolution of the plan to rearm Japan during the period 1950 to 1952, against the political background of escalation of Cold War tensions and the lead-up to the Korean War. In Chapter Four, 'Constitution Bans War', Kowalski details the events that led to the adoption of Japan's pacific constitution, in particular Article 9, which states:

Aspiring sincerely to an international peace based on justice and order, the Japanese people, forever, renounce war as a sovereign right of the nation, or the threat or use of force, as a means of settling disputes with other nations. In order to accomplish the aim of the preceding paragraph, land, sea, and air forces, as well as other war potential, will never be maintained. The right of belligerency of the state will not be recognized.

This uncompromising article lies at the heart of the heated debate that attended the Abe cabinet's approval of a limited re-interpretation of the constitution to allow the JSDF to engage in collective defence measures with close allies. Following the adoption of the constitution, the Japanese were forced to go to extraordinary lengths of euphemism to avoid the possibility of constitutional violations when they began to re-arm in the 1950s, under pressure from the US. For example, military hardware such as tanks were referred to by the innocuous title of 'special vehicles'.

Even now, the Japan Maritime Self-Defense Force's Hyuga-class helicopter-carrying ships are designated destroyers, although their specifications are more consistent with those of light aircraft carriers (at 13,950 tons compared to the US Navy's Arleigh Burke-class destroyers which displace 8,315 tons). Kowalski's conclusion to this key chapter foreshadows the recent controversy in Japan over changes to Article 9, where he noted (at page 44) that:

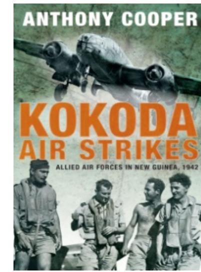
> [U]nder our prodding, the nation turned its back on this noble aspiration, marching over its constitution into an uncertain and confused future. In retrospect one wonders, why did we have to play God with these people?

Similarly perceptive comments permeate the text, which was edited and annotated by Robert D. Eldridge. His light editorial touch is another important aspect of *An Inoffensive Rearmament.* Eldridge, the deputy assistant chief of staff for Marine Corps Installations Pacific, worked with Kowalski's family to produce this first-ever English edition of the book. He is also a well-published academic with considerable experience in Japan and a deep understanding of Japanese history. As with many other history books, the importance of *An Inoffensive Rearmament* lies as much in its historical insights as it does in its contemporary resonance.

In the wake of the conflicts and stability operations of the past decade, Western nations have again taken on the task of rebuilding the security forces in a number of strife-torn nations—the armed forces and police in Iraq, the national police in the Solomon Islands, and the armed forces and police in Afghanistan are just three examples. The success of these ventures has been mixed, often due to communal tensions between religious and ethnic factions, factors that portend a poor outcome for the process in Afghanistan.

Although it dates from a different time and a different culture, *An Inoffensive Rearmament* demonstrates how such a difficult task can proceed with a degree of success yet to be attained by contemporary attempts at the same endeavour.

Kokoda Air Strikes: Allied Air Forces in New Guinea, 1942



Anthony Cooper
NewSouth Books: Sydney, 2014, 528 pages
ISBN: 978-1-7422-3383-3
$39.99

Reviewed by Kristen Alexander

Dr Anthony Cooper's second book, *Darwin Spitfires: the real battle for Australia*, well-deservedly received the Northern Territory Chief Minister's NT History Book Award. *Kokoda Air Strikes: Allied Air Forces in New Guinea, 1942,* his third book and second dealing with aspects of the RAAF's air war in the Second World War, also deserves accolades.

Here, Cooper casts a careful and occasionally—but understandably—cynical eye over the operations of the Allied air forces in the crucial New Guinea campaigns. He has taken on a formidable task. Rather than focus on specific topics, he offers a synopsis of existing Australian, Japanese and American research. Beginning with the conquest of Rabaul in January 1942, he presents the operations in the South West Pacific theatre—Coral Sea, Kokoda, Milne Bay and Guadalcanal—as a single air campaign.

Importantly, he takes it further and discusses the battle for New Guinea as part of a broader, interconnected land, air and sea campaign with significant contributions by both the RAAF and American air forces. He confidently acknowledges that some of his conclusions may be open to challenge and welcomes stimulating discussion.

In presenting a survey of significant operations within a campaign—and one of the best to my mind is the excellent 'Losing Lae and Salamaua' narrative—there is little place for individual stories. Indeed, the reader should not expect a human focus—the clue is in the title—and yet Cooper manages to include key vignettes which constantly reinforce the human cost of a campaign which had to contend with incomplete training, unsuitable aircraft and poorly set up and exposed airfields.

The opening story highlights the inadequacies and the sterling bravery of the men who carried out their duty despite exhaustion, sickness, poor morale and the possibility of capture and murder. Often, Cooper employs just the lightest touch in the briefest mention of a personal tribute to spotlight the legacy of continuing losses, such as Medical Officer Deane-Butcher's recovery of Sergeant Richard Granville's body from wreckage, and the Australian flag, woven by the women of Itikinumu Plantation, placed on his coffin.

Cooper presents a forthright and clearly articulated argument. If errors of judgment were made by commanders, he does not soft foot around them. He pulls no punches and thoroughly dissects their failures. This is a significant strength, as is his defence of commanders such as Lukis, Brett and Scanlon who have received unjust criticism by other commentators. As Cooper says, 'Credit where credit's due!' and his reassessments are soundly based and utterly fair.

Another highpoint is the selection of photos. The author's obvious commitment to sourcing high-quality photos, regardless of the cost, pays off. Rather than relegating them to a glossy photo block, which limits the number of inclusions, photos are incorporated into the text, thus illustrating the story they belong to. The high-resolution Australian War Memorial images allow for this. Poor-quality personal album pics would not have worked in this reader-friendly approach.

Complementing the 45 exceptionally well-chosen images are detailed captions which add more to the story and clearly demonstrate Cooper's broad knowledge of every aspect of this campaign: men, machines, equipment and terrain. Indeed, the breadth of Cooper's knowledge is impressive.

He ranges from aircraft specifications and ensuing strengths and limitations, through to pilots' living conditions and inadequate kit, to tactics and strategy, and high-level machinations and international relations.

Readers will want to consult this remarkable history time and again and happily NewSouth Books have an eye for presentation. The book is stitch bound so will survive frequent and hardy reading, and is on good-quality paper. The only downside is that it is a big volume and some publishing compromises had to be made. The main casualty was the source notes. (Cooper wryly refers to the dispassionate ruthlessness involved in fitting a campaign this size into one not-overlarge book.)

Happily, there is a good index and Cooper has not overlooked the fact that many readers want to springboard to further reading from authoritative accounts such as this. He has put glossary and extensive endnotes on his website <http://www.darwinspitfires.com/kokoda.html>. Maps and a formation summary, however, maintain their place in the book.

Kokoda Air Strikes: Allied Air Forces in New Guinea, 1942 is highly detailed, finely argued and a stimulating read. It canvasses the source material well and, with such well-reasoned analysis, may well be considered the new *de facto* official history of Australia's part in the New Guinea air campaign. Highly recommended.

A National Force: the evolution of Canada's Army, 1950-2000

Peter Kasurak
University of British Columbia Press: Vancouver, 2014, 350 pages
ISBN: 978-0-7748-2640-2
C$34.95

Reviewed by John Donovan

Dr Peter Kasurak, former leader of the defence and national security sections of the Auditor General of Canada, brings the eye of an informed outsider to this study of Canada's Army during the second half of the 20th century. His story highlights missed opportunities, substantial change being implemented only after the end of the Cold War, and several scandals.

According to Kasurak, the first missed opportunity was immediately after the Second World War when Lieutenant General Charles Foulkes became Chief of the General Staff. He favoured a modernised officer corps, drawing on civilian university graduates receiving post-graduate training at the Royal Military College of Canada. His successor recommended lower education standards for officers.

In the late 1960s, an Officer Development Board was established, reporting to General Jean-Victor Allard, Chief of the Defence Staff. It proposed a number of changes, including the delegation of tactical responsibility to NCOs to reduce the number of officers, and that officers should be recruited from the top 15 per cent of school leavers, with a high proportion holding degrees. However, the Board and its recommendations lapsed with Allard's retirement. Reform of the Canadian officer corps was then delayed until the 21st century, when the aim of a tertiary-educated officer corps was largely achieved by 2009.

An opportunity for substantial organisational change came when Major General Roger Rowley was appointed to command 1 Canadian Infantry Division in 1962. He proposed such innovations as brigade service battalions, and conducted 'function studies' of arms elements, which pointed towards combining armour and infantry in tactical units for high-intensity warfare.

These proposals were overtaken by a short-lived move to a 'mobile force', and integration (and later unification) of the Canadian Forces. Masurak describes the extended process under which the Army developed plans for a mobilised force of one to two corps, focused on attrition rather than manoeuvre. Decades were spent pursuing this goal, which took little account of the likely availability of resources, equipment or personnel.

Between occasional attempts to develop strategically-transportable general purpose forces, and despite continuing government priority for the defence of Canada, the Army remained focused on the mechanised brigade commitment to NATO's Central Front, which absorbed massive resources. Although the combat development staff in 1979 prepared a paper advocating a more realistic objective, planning for a 'big army' continued until around 1990.

The 'big army' Corps 96 (a reduced version of the earlier Corps 86) was abandoned in the 1990s, although the 1987 Defence White Paper had breathed short-term life into it. The Army's Combat Development Guide was withdrawn, with the caveat that 'the army need[s] to balance requirements against available funds'. After decades preparing for high-intensity war in Europe, Kasurak describes how a brigade was not ready to fight in the 1990-91 Gulf War, only a couple of years after the end of the Cold War.

Canada's military had sought unachievable targets, including equipment beyond the capabilities of current technology. 'Development guided by realism' was not a popular option but the end of the Cold War and financial cutbacks enforced it.

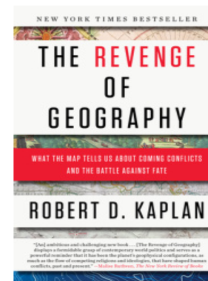
Kasurak also contends that the role of Canada's part-time militia was never resolved. The regulars sought a large militia order-of-battle as the basis for a 'big army', ignoring numbers, training states, readiness and equipment deficiencies. Senior militia officers sought an independent role, ignoring those same constraints. For a short period in the late-1950s and 1960s, the militia had a role as post-nuclear recovery force, before lapsing back into habit as part of the 'big army' ambition. While its primary role became to augment and sustain the regular units, its force structure was maintained but with no mobilisation plan.

The 1990s was a 'decade of darkness' for the Canadian Army. In an important chapter, Kasurak describes failures in discipline and ethics that plagued the Canadian Army, culminating in the murder of a Somali youth and disbandment of the Canadian Airborne Regiment. After major budget reductions, Canadian Forces Europe was disbanded. Its heavy equipment was redistributed to establish three brigade groups in Canada, each combining heavy tracked and lighter wheeled vehicles. Development of a 'multi-purpose combat capable force' commenced.

Kasurak highlights the relationship between the government and the military as 'principal' and 'agent' in which, once the military agent's advice has been tendered and considered, the agent must follow the requirements of the civilian principal. He sees ignoring this relationship as a major failure in the evolution of Canada's military forces over this period.

This book has important lessons for armies facing imprecise threats with limited resources, and should be widely studied in Australia.

The Revenge of Geography: what the map tells us about coming conflicts and the battle against fate



Robert D. Kaplan
Random House: New York, 2013, 346 pages
ISBN: 978-0-8129-8222-0
US$16.99

Reviewed by Brigadier Chris Field, CSC, Australian Army

> Geography, geopolitics, and geostrategy have been imprudently neglected by students of strategy for more than half a century.
>
> Colin S. Gray, *Perspectives on Strategy,* 2013, p. 202

Heeding Professor Gray's admonishment, ADF military professionals can utilise Robert Kaplan's *The Revenge of Geography* to expand their thinking and diversify their conceptual understanding of geography, geopolitics and geo-strategy. Kaplan is chief geopolitical analyst for STRATFOR, a private global intelligence firm, and the author of some 14 books, including *Monsoon: the Indian Ocean and the future of American power* and *Warrior Politics: why leadership demands a pagan ethos*.

Kaplan's thesis on geography, geopolitics and geo-strategy is that:

> [T]he only thing enduring is a people's position on the map. Thus, in times of upheaval maps rise in importance. With the political ground shifting rapidly under one's feet, the map, though not determinative, is the beginning of discerning a historical logic about what might come next.

Kaplan explains that geography, derived from Greek and meaning 'a description of the earth', has often been associated with fatalism and therefore stigmatised; 'for to think geographically is to limit human choice'. However, Kaplan argues that 'the more we remain preoccupied with current events, the more that individuals and their choices matter; but the more we look out over the span of centuries, the more geography plays a role'.

Kaplan supports his thesis when he predicts the 2014 Russian intervention in Ukraine. He explains that Ukraine means 'borderland' and is a country with 'unremitting and unimpeded steppes … [which] lacks natural boundaries and is drained by relatively few navigable rivers'. He contends this means the Ukraine's 'flatness, continentality, and migration routes lead to conflict and swift changes of fortune'.

Kaplan states that President Putin's concentration on Ukraine is 'proof of his desire to anchor Russia in Europe, albeit in non-democratic terms'. He asserts that Ukraine is a pivot state that in and of itself transforms Russia. Moreover, Ukraine's very independence keeps Russia to a large extent out of Europe. Kaplan concludes that without Ukraine, Russia can still be an empire but would be a 'predominantly Asian' one, drawn further into conflicts with Caucasian and Central Asian states. However, with Ukraine back under Russian domination, Russia would add 46 million people to the western portion of its demography and more directly challenge Europe, even as it is integrated into it.

Kaplan frequently quotes geopolitical theorists who, alongside military theorists such as Thucydides, Clausewitz, Jomini, Sun Tzu, Mao Zedong, Mahan, Corbett, Douhet, Trenchard and Mitchell, deserve serious study by ADF professionals. These theorists and their key ideas are:

- Hans Morgenthau (political realism)
- John Mearsheimer (offensive realism)
- Halford Mackinder (the Eurasian heartland)
- Nicholas Spykman (the so-called rimland)
- Marshall Hodgson (the Oikoumene or 'Nile-to-Oxus'), and
- William Hardy McNeill (all cultures acted on and were acted on by others).

The Revenge of Geography is essential reading for ADF professionals. Kaplan's work is expansive and thought-provoking. In particular, Kaplan places Australia's geopolitical position in context supported by theoretical analysis, historical examples and global realities. Most importantly, *The Revenge of Geography* expands the lens for Australians, and members of the ADF, to see ourselves. It is a timely enhancement to Australia's 21st century strategic thinking.